Department of Defense Healthcare Management System Modernization (DHMSM) Program

Attachment 1: IDIQ PWS

DHMSM Program Management Office
DoD Healthcare Management Systems (DHMS) Program Executive Office

Solicitation Number: N00039-14-R-0018

DISTRIBUTION LIMITATION
Distribution Statement A: Approved for public release; distribution is unlimited.

Table of Contents

1 Overview 1
1.1 Background 1
1.2 EHR System Operational Capability 1
1.3 DHMSM Program Execution 3
1.3.1 System Engineering 3
1.3.2 Testing 4
1.3.3 Deployment Services 4
1.3.4 Sustainment 6
1.4 Contract Execution 6
2 Scope 7
3 Applicable Documents 7
4 Performance Details 8
4.1 Place of Performance 8
5 Services and Deliverables 9
5.1 Program Management 9
5.1.1 Contractor Facilities 10
5.1.2 Key Personnel 10
5.1.3 Meeting Attendance/Support 12
5.1.4 Product Demonstration 13
5.1.5 Reporting Requirements 14
5.1.6 Quality Management 16
5.1.7 Risk Management 17
5.1.8 Schedule Management 17
5.1.9 Management of Government Property 18
5.1.10 Security Management 19
5.1.11 Transition Planning 32
5.2 Enterprise Electronic Health Record (EHR) System 33
5.2.1 Open System Architecture 34
5.2.2 Software Requirements 35
5.2.3 Hardware Requirements 36
5.2.4 Engineering Site Visit and Analysis 37
5.2.5 System Design 39
5.2.6 System Configuration & Integration 43
5.2.7 System Installation 45
5.2.8 Continuity of Operations (COOP), Disaster Recovery (DR), and Business Continuity Planning Services 45
5.2.9 System Quality and Performance Measures 46
5.3 Change Management 47
5.3.1 Business Process Reengineering 47
5.4 Training 48
5.4.1 Virtual Training Environment 48

5.4.2 Learning Management System 49
5.5 Systems Engineering 49
5.5.1 Engineering SETR, Milestone and Review Support 50
5.5.2 Systems Engineering Processes 51
5.5.3 Requirements Management 54
5.5.4 Configuration Management 54
5.5.5 Release Management 55
5.5.6 Data Management 55
5.5.7 Cybersecurity 56
5.5.8 System Safety 59
5.6 Testing 60
5.6.1 Testing Meetings 61
5.6.2 Integration and Test Lab Environment 61
5.6.3 Configuration and Integration Testing 62
5.6.4 Developmental Test and Evaluation 63
5.6.5 Operational Test and Evaluation 64
5.7 Deployment Services 64
5.7.1 Deployment Site Visit 65
5.7.2 Segment 1 Training 65
5.7.3 Segment 2 Training 66
5.7.4 Segment 1 Deployment 66
5.7.5 Segment 2 Deployment 67
5.8 Sustainment 68
5.8.1 Software Maintenance 69
5.8.2 Hardware Maintenance 69
5.8.3 Product Improvement Engineering 70
5.8.4 Software and Hardware Refresh 70
5.8.5 Operations and Monitoring 70

List of Tables

Table 3-1 DHMSM PWS Applicable Documents 7
Table 5-1 Key Personnel 11

1 Overview

1.1 Background

The Department of Defense (DoD) Military Health System (MHS) has multiple legacy healthcare systems and data stores, developed over decades, which need to be modernized. This modernization must ensure and enable sustainability, flexibility, and interoperability of the MHS while improving the continuity of patient care. The DoD Healthcare Management System Modernization (DHMSM) program was established to support the May 21, 2013 Secretary of Defense (SECDEF) memorandum mandating DoD to competitively select a configurable, scalable, and modernized Off-the-Shelf (OTS) Electronic Health Record (EHR) System. The EHR System will replace MHS legacy clinical systems including, but not limited to, the Armed Forces Health Longitudinal Technology (AHLTA), Composite Health Care System (CHCS), and most components of the Theater Medical Information Program-Joint (TMIP-J). The National Defense Authorization Act of Fiscal Year (FY) 2014 mandates that the EHR System be deployed by December 31, 2016. When implemented, the EHR System will provide access to authoritative clinical data sources, and over time become the authoritative source of clinical data to support improved population health, patient safety, and quality of care to maximize medical readiness for the DoD.

As directed by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) Acquisition Decision Memorandum (ADM) of June 21, 2013, the DHMSM Program Management Office (PMO) was chartered to manage the acquisition and implementation of the OTS EHR System. The contractor, also referred to as the Service Provider/Integrator (SPI), will deliver an EHR System for deployment across the DoD enterprise as well as the associated management, engineering, testing, deployment, and sustainment services. The contractor will provide an integrated inpatient/outpatient Best of Suite (BoS) solution, augmented by Best of Breed (BoB) products to meet the DoD approved requirements. BoS refers to an integrated inpatient and outpatient solution with software components that have been designed, integrated, maintained, and deployed with a design architecture that allows for access to and sharing of common data, common user interfaces, common workflows, and common business rules, and that supports end-to-end healthcare related clinical and business operations. BoB is defined as a solution or module not considered part of the BoS, which would require engineering and integration efforts in order to be incorporated into the BoS.

The DHMSM PMO will deploy an OTS EHR system through system configuration, integration, and, if required, limited custom tailoring. Some software modifications may be made to enable accurate interface activity among legacy support systems and the EHR System. It is expected that existing network(s) and infrastructure will be utilized, as much as practicable, to support any proposed solution.

1.2 EHR System Operational Capability

The Government Requirements Traceability Matrix (RTM) defines the technical parameters to enable the EHR System to support DHMSM functional capabilities. The EHR System will meet all of the functional and non-functional requirements, including the Critical Success Factors (CSFs) among other performance measures and objectives, identified in the Government RTM (Attachment 2). The DHMSM functional capabilities are derived from the following Concept of Operations (CONOPS) (hereinafter the “approved CONOPS”):

a) Health Readiness CONOPS, 21 January 2010 (Attachment 10)

b) Force Health Protection CONOPS, 17 November 2011 (Attachment 11)

c) Health Service Delivery CONOPS, 22 February 2011 (Attachment 8)

d) Health System Support CONOPS, 22 February 2011 (Attachment 9)

The EHR System requirements are established at a strategic level and will guide the configuration and implementation of the system in the MHS enterprise. In addition to the requirements in the Government RTM, the Government may place orders for product enhancements or improvements to meet emerging needs, activate existing, but dormant capabilities in the EHR system solution, or to address a need in the approved CONOPS not explicitly extrapolated into the Government RTM.

The EHR System is expected to unify and increase accessibility of integrated, evidenced-based healthcare delivery and decision-making. The EHR System will support the availability of longitudinal medical records for 9.6 million DoD beneficiaries and approximately 153,000+ MHS personnel globally. MHS personnel include activated members of the National Guard and Reserve, estimated at 50,000 additional personnel. Members of the National Guard and Reserve are typically activated about one month out of the year. The EHR System will enable the application of standardized workflows, integrated healthcare delivery, and data standards for improved and secure electronic exchange of medical and patient data between the DoD and its external partners, including the Department of Veterans Affairs (VA), and other Federal and private sector healthcare providers. The workflows inherent to the EHR System will be adopted by and standardized throughout the MHS via the DHMSM Change Management process, as applicable. The EHR System will leverage data exchange capabilities in alignment with the Interagency Program Office (IPO) for standards-based health data interoperability and secure information sharing with external partners to include the VA.

The DHMSM PMO has established two segments to support deployment of the EHR System to the MHS enterprise, serving all Active duty, Reserve, Guard, and beneficiaries. Segment 1 will deploy the EHR System to all medical and dental permanent fixed facilities worldwide, inclusive of approximately 55 Inpatient Hospitals and Medical Centers, 361 Ambulatory Care Clinics, and 249 Dental Clinics. Segment 2 will work with the Deployment and Readiness Systems (D&RS) Program Office, which manages TMIP-J, and the Services' infrastructure program offices, to deploy the EHR System to permanent and temporary operational environment platforms to meet capabilities required for each Role of Care, as defined in Joint Publication 4-02 Health Service Support. Operational platforms currently include 225 ships, 75 submarines, and 2 hospital ships; temporarily deployed operational medical units currently include approximately 6 Theater Hospitals, 450+ Forward Resuscitative Sites, 3 Aeromedical Staging Facilities (ASF) and numerous aeromedical evacuation teams to support military operations abroad. The contractor will deliver an EHR System and related services to a complex, geographically dispersed, global enterprise in an extremely dynamic environment.

Segment 2 capabilities must function in a low/no communication environment, in support of the Roles of Care defined below:

a) Role 1 - first responder capabilities including immediate lifesaving measures

b) Role 2 - forward resuscitative care including advanced trauma/emergency medical treatment. Some Role 2 sites are expanded to include additional medical services and Ancillary support services (e.g., Laboratory, Pharmacy, Radiology) to provide more robust care for larger Patient at Risk (PAR) populations. Expanded sites are detailed in Attachment 13, Segment 2 Roles of Care and Descriptive Statistics

c) Role 3 - theater hospitalization including robust care for resuscitation, surgery, and post-operative care
d) EnRoute Care - care required to maintain the phase treatment initiated prior to evacuation and the sustainment of the patient's medical condition during evacuation. Care can range from in-flight skilled nursing care up to invasive Critical Care services from Critical Care Air Transport Teams (CCATT)

1.3 DHMSM Program Execution

1.3.1 System Engineering

The contractor will conduct site visits to initiate the EHR System development lifecycle. Preliminary designs, architectures and system requirements will be validated, extended, and derived as the result of onsite analysis of Military Treatment Facilities (MTFs) and mock-ups of medical operational environments. Operations and infrastructure analysis will be structured to obtain detailed system workflows (use cases), data exchanges, and their dependencies to system interfaces. These inputs will be used to refine system design, enterprise architecture and system integration requirements. Gap analysis will be conducted to extend existing requirements and derive new requirements to inform the system deployment strategy. Gap analysis will result in additional functional, technical or programmatic refinement of the system design and System Subsystem Specification (SSS) for review and approval during Initial Design Review (IDR).

During IDR, the contractor will demonstrate to the Government that the system requirements are fully allocated, are traceable to critical system functions, and the design addresses all technical risks, and will meet all requirements. The contractor's Integrated Master Schedule (CIMS) will identify the critical Configuration and Integration Testing (CIT) events required to align the system workflows, interfaces, data, security and infrastructure capabilities needed to test and verify the DHMSM design, mitigate engineering risks and continually assess DHMSM technical measures.

The System Subsystem Design Document (SSDD) will identify critical functional and technical capabilities, the associated risks and necessary mitigation activities. The CIMS will identify In Process Reviews (IPRs) required to continually assess technical risk, system performance and quality. To be successful, this method requires close alignment with the appropriate DHMSM Technical Working Group (WG), IPO for data standards, Defense Medical Information Exchange (DMIX) program office for enterprise integration, Medical Community of Interest (Med-COI) for network and infrastructure program, and the Defense Health Agency's (DHA's) portfolio of clinical and business systems.

The EHR System's data will comply with the current DoD Net-Centric Data Strategy (NCDS), conveying the data management activities that must take place to enable net-centric concepts. The focus of the NCDS is to make data visible, understandable, trusted, interoperable, computable, and responsive to user needs. It also conforms to emerging DoD level net readiness standards (e.g., data strategy, transport, applications, etc.). The NCDS activities serve as a guide to architects and program managers in establishing and maintaining the net-centric data foundation for their enterprise. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a net-centric military capability.

Requirements Management provides vertical and horizontal traceability back to user-defined capabilities as documented through the approved CONOPs documents. Requirements

Management also encompasses obtaining an understanding of requirements, obtaining a commitment to requirements, and identifying inconsistencies between project work and requirements. The DHMSM program will maintain traceability of all the requirements from the capabilities needs, to documenting the changes to the requirements, and recording the rationale for those changes in accordance with the PEO Requirements Management Plan.

DHMSM PMO will adhere to the Configuration Management (CM) policies and practices as described in the PEO Configuration Management Plan. CM includes supporting the definition of Configuration Items (CIs) and relevant attributes and relationships to manage, establishing procedures for change and controlling request for change, providing the status of the CIs, and auditing the actual and authorized versions of each item. Maintaining a complete and accurate CM system ensures the integrity of system/software baselines and designated CIs required to provide services.

1.3.2 Testing

Test activities will be conducted in Government-Approved Labs (GALs) that represent operationally and technically realistic test environments and mockups to support the testing of the EHR system. By emulating the working conditions of clinical end-users, the GALs will enable a realistic view of how effective the performance of the EHR System will be in production. The contractor will install and operate the EHR System in the GALs to support all testing activities.

The EHR System will undergo a series of testing by the contractor, a Government Independent Test and Evaluation (T&E) team, and Operational Test Agencies (OTAs). The contractor will conduct Configuration and Integration Test (CIT) to verify all DHMSM requirements have been met. In order to support Developmental Test and Evaluation (DT&E), the Test Readiness Review (TRR) must be completed no later than ten (10) months after Task Order award. During DT&E, Independent Government test agencies verify and validate the EHR System in the GAL. Systems Integration Testing (SIT) will verify that the integrated systems meet the interface requirements and work as required. Performance testing will assess thresholds and limitations of the system for all hardware, software and network components. Functional testing will verify key technical and functional system characteristics, based on the critical success factors identified in the Government RTM.

After the Limited Fielding for Initial Operational Capability (IOC) Authority to Proceed (ATP) decision, the Government will conduct Operational Test and Evaluation (OT&E) at the IOC sites for Segment 1 and Operational Medicine Mockup for Segment 2. OT&E will be conducted in three phases; the first two phases will use synthetic patient data for both Segment 1 and 2, while the third phase will use live patient data for Segment 1. Successful completion of OT&E Phase 3 completes testing for Segment 1. Successful completion of OT&E Phase 2 completes testing for Segment 2.

1.3.3 Deployment Services

1.3.3.1 Change Management

A vital aspect of successful EHR System implementation is the planning and execution of change management activities. The contractor will conduct site visits at all MTFs throughout the implementation process to assess facility leadership understanding of, preparation for, and acceptance of the new EHR. The DHMSM PMO, DHA, D&RS, and the contractor will collaborate to define enterprise workflows within the EHR System. The contractor will perform gap analyses at each site between the “As-Is” and “To-Be” workflows. The contractor will customize training based on the gap analyses to facilitate user adoption. The contractor will

solicit communications preferences and best practices, and training lessons learned from the MTFs.

1.3.3.2 Deployment

Deployment is defined as the implementation of all hardware and software, user documentation, site survey, site activation, user training, data migration, management, engineering support, and interim logistics support related to the MHS enterprise sites. For Segment 1, the term Go-Live, for IOC, is defined as successful completion of DT&E and achieving the Limited Fielding for IOC ATP. During Full Deployment (FD) to the enterprise, the term Go-Live is defined as successful completion of the Operational Readiness Review (ORR) exit criteria. For Segment 2, TMIP-J and the Services infrastructure program offices will implement the EHR System in the Operational Medicine environment(s).

DHMSM PMO has constructed an MTF Code, which the contractor will use to plan and execute the implementation and deployment of the EHR System. The MTF Code characterizes sites, provides a standardized format and common language for MTF sites, provides clarity on the clinical services available at each site, and provides high-level descriptors to provide additional technical clarity at each site.

IOC is the first major production event that proves EHR System success. IOC is completed for Segment 1 when all designated IOC Sites have completely transitioned to the EHR System and no longer rely on the MHS legacy systems for day-to-day operations, with the exception of access to historical patient information. Segment 2 achieves IOC at the completion of OT&E Phase 2.

Following successful completion of IOC for Segment 1 the EHR System will be deployed in a Waves construct to the remaining MTFs and Dental Facilities. Once all MTFs are fully transitioned to the EHR System, FD is achieved. For Segment 2, FD is achieved when the EHR System Gold Disk has been delivered to TMIP-J and the Services.

The contractor will provide Post Go-Live On-Site Support (OSS) activities up to 90 days at all MTF locations. Post Go-Live support activities include, but are not limited to, providing 24/7 over-the-shoulder support, troubleshooting system issues, and assisting end-users with workflow support by mapping and gapping the new business processes.

1.3.3.3 Training

The contractor will employ training methodologies specific to the DoD environment and workflows that will meet the needs of Segments 1 and 2 end-users, as well as, medical facilities' needs based on information obtained during deployment site visits. Training methodologies will include: instructor-led classroom, instructor-led virtual, computer-based training (CBT), and over-the-shoulder training.

For Segment 1, the contractor will be responsible for providing training to the medical facilities' trainers, as well as, end-users (functional, technical, and administrative). Training for clinical champions, super users, and local trainers will begin at least 90 days prior to Go-Live. Instructor-led training (ILT) for end-users will start at least 60 days prior to Go-Live and will end approximately 1 week prior to Go-Live to ensure optimal knowledge retention. The contractor will provide Over-the-Shoulder training to end-users for at least 90 days post Go-Live. "Train-the-trainer" (T3) training for Segment 1 will include clinical champions, super users, and local trainers.

For Segment 2, training for designated TMIP-J and Service personnel will consist of a train-the-trainer approach. The objective is to qualify TMIP-J and Service personnel to train Operational Medicine end-users and administrators on EHR System for Segment 2.

The contractor will provide training for DHA Global Service Center (DHAGSC) staff and provide training to Government testers (technical/functional Subject Matter Experts (SMEs)) to support testing activities.

1.3.4 Sustainment

The contractor shall provide all services and material necessary to perform sustainment of the EHR System. Sustainment must be in place to support all Government testing for Segment 1 and Segment 2. Sustainment includes test items (e.g. test scripts, test cases, test data sets, interface emulators) necessary to support the Configuration Control Board (CCB) with regression testing. Sustainment must continue after MTF Go-Live for Segment 1 and delivery and acceptance of the EHR System Gold Disk for Segment 2.

The DHAGSC will provide functional and technical support for the EHR System incidents. Incident troubleshooting will be handled by local IT support and DHAGSC. For Segment 1, trouble tickets not resolved at DHAGSC Tier 2 will be escalated to Tier 3. For Segment 2, specific software problem/incident that cannot be resolved at Tier 2 will be routed to TMIP-J Tier 2.5. The tier structure is defined in the DHMSM Deployment, Training & Change Management Plan (DTCMP). The contractor will receive, analyze, and resolve all assigned Tier 2.5 and Tier 3 trouble tickets.

The contractor will provide software and hardware maintenance and support for the EHR System at all locations. The contractor will ensure that software and hardware maintenance requirements are met. Maintenance consists of upgrades, correcting faults, modifications improving performance or other attributes, and adapting to a changing organization and technical environment. Corrective maintenance will accommodate defects as reported by users. Enhancements or improvements to the EHR System will be submitted by the contractor to the DHMSM PMO and subsequently the Configuration Control Board (CCB) for approval.

1.4 Contract Execution

This contract is an Indefinite Delivery/Indefinite Quantity (IDIQ). The IDIQ contract defines the overall contract delivery requirements. Task Orders will be issued that define specific tasks, services, and Contract Data Requirements List (CDRL) items that the contractor must deliver in support of the IDIQ contract. The total potential ordering period for this effort is ten (10) years, consisting of a two-year base ordering period and two subsequent option ordering periods, consisting of three (3) years each to allow for deployment Task Orders from post-IOC through FD. The Period of Performance (PoP) will also include the potential for an award term consisting of up to 24 months for sustainment support post-FD, which may be awarded based on the performance criteria in the Award Term Plan.

Task Orders will contain independent Quality Assurance Surveillance Plans (QASPs) that define the performance standards upon which contractor performance will be measured. Task Order 0001 requires the contractor to design, integrate, and configure the EHR System to meet or exceed the requirements necessary for a successful DT&E. Task Order 0002 requires the contractor to support OT&E activities and execute deployment, change management, and training activities in order to successfully meet the IOC schedule and requirements.

Successive Task Orders will be executed requiring the contractor to provide deployment, change management, training, engineering, configuration management, sustainment, and other

activities to support enterprise deployment of the EHR System to the remaining Segment 1 sites. For Segment 2, Task Orders will be issued requiring the contractor to provide engineering and configuration management support to deployment activities and training. In addition, sustainment Task Orders will be issued to enable the enterprise sustainment and maintenance of the EHR System over the program lifecycle, through FD.

2 Scope

The contractor will provide an OTS EHR System for deployment across the DoD enterprise. The contractor will support integration, configuration, testing, deployment, training, and sustainment for the EHR System. The EHR System will replace functionality of core legacy systems, and will be deployed to both fixed and Operational Medicine treatment facilities.

All time frames listed in this IDIQ PWS are calendar days unless otherwise stated.

3 Applicable Documents

Table 3-1 DHMSM PWS Applicable Documents

DHMSM PWS Applicable Documents	
1.	DoD 5200.2-R, “Personnel Security Program,” current version
2.	DoD Instruction 8500.01, “Cybersecurity”, March 14, 2014
3.	The DoD Open System Architecture (OSA) Contract Guidebook for Program Mangers, Version 1.1, June 2013
4.	DoD Directive 8530.1, “Computer Network Defense (CND)”, January 8, 2001
5.	DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT)”, March 12, 2014
6.	MIL-STD-882E “Department of Defense Standard Practice System Safety” May 11, 2012
7.	DoD Instruction “Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense” (DODI 8320.02), issued August 5, 2013
8.	OMB Circular A-130, Management of Federal Information Resources (November 28,2000)
9.	National Institute of Standards and Technology: Federal Information Processing Standards (FIPS) http://www.nist.gov/itl/fipscurrent.cfm
10.	DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property, May 19, 2011
11.	MIL-STD-130N, DoD Standard Practice Identification Marking of US Military Property, 16 November 2012
12.	MIL-STD-881C, Department of Defense Standard: Work Breakdown Structures (WBSs) For Defense Materiel Items, October 3, 2011
13.	Joint Publication (JP) 4-02, Health Service Support, July 26, 2012
14.	DoD 5000.04-M-1 Cost and Software Data Reporting (CSDR) Manual, November 4, 2011
15.	American National Standards Institute / Electronic Industries Alliance (ANSI/EIA) 748C, March 2013
16.	Health Information Technology for Economic and Clinical Health Act, Feb 17, 2009
17.	DoD Joint System Safety Engineering Handbook
18.	PEO Risk Management Plan
19.	DHMSM Deployment, Training, Change Management Plan

DHMSM PWS Applicable Documents	
20.	DHMSM Engineering Master Plan
21.	DHMSM Test Strategy
22.	DHMSM Government Approved Labs Plan
23.	PEO Configuration Management Plan
24.	PEO Requirements Management Plan
25.	PEO Cybersecurity Strategy
26.	PEO Data Management Strategy
27.	PEO Release and Deployment Management Plan
28.	DHMSM Data Communications Network and Enterprise Services Infrastructure Framework
29.	DHMSM Interface Strategy
30.	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 25010:2011, March 1, 2011
31.	DoD AI-15 OSD Records and Information Management Program, May 3, 2013
32.	DoD Manual 5220.22M National Industrial Security Program Operating Manual (NISPOM), February 28, 2006
33.	Directive-Type Memorandum (DTM) 08-003, “Next Generation Common Access Card. (CAC) Implementation Guidance,” December 1, 2008
34.	DoDI 8500.2, Information Assurance (IA) Implementation, February 6, 2003
35.	DISA Approved Product List (https://aplits.disa.mil/processAPList.do)
36.	ISO/IEC 12207 IEEE Std. 12207-2008, Second edition 2008-02-01, “Systems and software engineering – Software life cycle processes”
37.	Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
38.	Form I-9 “Employment Eligibility Verification” (http://www.uscis.gov/files/form/i-9.pdf) in OMB No. 115-0136
39.	DoD 8570.01-M, December 19, 2005
40.	DoD Directive 5205.02E, June 20, 2012
41.	Office of Management and Budget (OMB) Memorandum 99-05, Attachment B
42.	DoD Privacy Impact Assessment (PIA) Guidance, February 12, 2009
43.	DD Form 2930, November 2008
44.	DoD 5400.11-R, "DoD Privacy Program", May 14, 2007
45.	DoDI 5200.44, November 5, 2012

4 Performance Details

4.1 Place of Performance

Performance under this contract will require work to be performed at Government and contractor facilities, including but not limited to:

a) Permanent fixed facilities [Continental United States (CONUS) and Outside Continental United States (OCONUS) in Asia and Europe] as identified in the Segment 1 List and MTF Codes (Attachment 12)

i. Inpatient Hospitals and Medical Centers
ii. Ambulatory Care Clinics
iii. Dental Clinics

b) Service Training Facilities
c) Government-Approved Labs (GALs)
d) D&RS Program Office, Services Infrastructure Program Offices and Training Facilities
e) Defense Information Services Agency (DISA) Enterprise Computing Centers (DECCs)
f) Contractor facilities

Specific places of performance will be identified in individual Task Orders issued under the contract. The contractor shall comply with host nation agreements for performance of any work in OCONUS locations and as specified in individual Task Orders.

5 Services and Deliverables

5.1 Program Management

Program Management provides the personnel, processes, and tools necessary to effectively manage the DHMSM program within schedule, quality, and performance requirements. Program support may require significant coordination and interfacing with various DoD and non-DoD activities located in CONUS and OCONUS.

The contractor shall:

a) Provide Program Management personnel, processes, documentation, and tools necessary to effectively manage the EHR System solution implementation within schedule, quality, and performance requirements
b) Establish and maintain a formal program management organization
c) Designate a Program Manager (PM) and Deputy PM empowered to make program and project level decisions and commit resources necessary to successfully execute courses of action within the scope of this contract
d) Develop a Program Management Plan (CDRL A001) that describes the following:
    i. Organizational Structure
        a. Organization diagram
        b. Directory with the positions, names, and contact information of all engineering, operations, and program management personnel on the DHMSM effort
    ii. Program Management Methodology
    iii. Subcontract Management Methodology
    iv. Performance Management Methodology
    v. Risk Management Methodology
e) Enter into Associate Contractor Agreements (ACAs) for any portion of the contract requiring cooperation and coordination (with contractors under other Department of

Navy, DoD, or DHA contracts) in the accomplishment of the Government's requirement at direction of the Government. The agreements shall include the basis for sharing information, data, technical knowledge, expertise, and/or resources essential to the implementation of DHMSM. "Associate contractors" shall be identified on individual Task Orders as required.

5.1.1 Contractor Facilities

The contractor shall establish new or utilize existing facilities as described below to facilitate coordination with the Government. The contractor's facility is not necessary for the exclusive use of this contract and can be utilized on a shared basis. The contractor facilities shall include sufficient physical security to protect government assets and information as required in DoD Manual 5220.22M (NISPOM), the terms and conditions of the contract, and this PWS.

5.1.1.1 National Capital Region (NCR) Facility

The contractor shall maintain a facility within 15 miles of the DHMS PEO located at 1700 N. Moore St. Arlington, VA 22209 within 60 days after issuance of the Task Order. Facility space shall include multiple conference rooms with audio/visual capabilities to accommodate the meetings described in section 5.1.3.

5.1.1.2 Puget Sound Facility

The contractor shall maintain a facility within a 50 mile radius of the Madigan Army Medical Center (MAMC) located at 9040 Fitzsimmons Drive, Tacoma, WA 98431 within 60 days of contract award to support the activities in Task Orders 0001 and 0002.

5.1.1.3 Facilities in Support of Wave Deployments

A portion of work under this contract will require close liaison with the Government in support of Wave deployments. The contractor shall establish a local facility when required by the Task Order.

5.1.2 Key Personnel

The contractor shall:

a) Assign to this contract those key personnel listed in table below. No substitutions shall be made except in accordance with the terms below

b) Agree that during the first 180 days of the contract performance period no key personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Procuring Contracting Officer (PCO) and provide the information required by paragraph (c) below. After the initial 180 day period, all proposed substitutions must be submitted in writing, at least 15 days (30 days if a security clearance is to be obtained) in advance of the proposed substitutions to the PCO. These substitution requests shall provide the information required below

c) Requests for approval of substitutions under this contract must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the PCO or needed by him to approve or disapprove the proposed substitutions. The PCO or an authorized representative will evaluate such

requests and promptly notify the contractor of his approval or disapproval thereof in writing

Table 5-1 Key Personnel

Key Personnel	Responsibilities
Program Manager	Maintains overall programmatic (cost, schedule, performance) responsibility for the execution of the contract and the delivery of services
Chief Engineer	Manages all engineering-related processes and projects while in the engineering phase. Manages a team of Engineers with expertise in areas such as Cybersecurity, Network Infrastructure, Client Engineering, Access Control, and Software
Clinical Informaticist	Assists in the optimization of the EHR System in support of the clinical, business, and Operational Medicine mission of the DoD. Responsible for EHR System workflow analysis, configuration and optimization, clinical content development, and user adoption Minimum competency requires demonstrated clinical informatics experience of at least 5 years, a Master's degree or higher in an informatics-related field, and at least 5 years demonstrated experience implementing, training, and optimizing the contractor EHR to support an integrated inpatient/outpatient health system network.
Physician Clinical Champion	A board-certified, actively practicing physician who provides support for EHR System workflow configuration and optimization, clinical content development, clinical decision support, training, user adoption, and change management. Minimum competency requires at least 5 years demonstrated experience implementing, training, optimizing, and using an EHR System to support an integrated inpatient/outpatient health system network.
Cybersecurity Manager	Manages all security-related processes; responsible for the overall security of the EHR System; service owner for all Cybersecurity-related services and solutions

Key Personnel	Responsibilities
Security Officer	Administers and assures compliance with security regulations and procedures in accordance with Contract guidelines at a Group or Large Legal Entity Level within the Division. Serves as the central focal point of contact for contractor security matters and shall have broad experience in all aspects of the security disciplines including personnel, physical, operations, industrial, communications, information, and information technology security. Directs and advise all departments regarding security regulations and procedures. Routinely interacts with Government agencies relative to security matters
Deployment Manager	Manages and directs the EHR System deployment. Responsible for defining and developing deployment plans, schedules, standards and procedures. Knowledgeable of the Department of Defense and the Military Healthcare System
Training Manager	Manages all training processes, identifies training needs, and resolves training problems. Provides expertise in support of training operations of the EHR System. Recommends solutions to ensure the effectiveness of the DOD health care delivery to optimize productivity and efficient utilization of resources

5.1.3 Meeting Attendance/Support

The contractor shall:

a) Host and participate in quarterly Program Management Reviews (PMRs) and monthly Progress Reviews

   i. Prepare a Meeting Agenda (CDRL A002), Presentation Materials (CDRL A003), and Meeting Minutes (CDRL A004)

   ii. Designate the appropriate SMEs to attend the PMRs and address agenda items

b) Meet with the PCO, Contracting Officers Representative (COR), and other Government personnel, as appropriate, to review the contractor's performance

c) Participate in Risk Management activities and meetings

5.1.3.1 Kickoff Meetings

Kickoff meetings are required for the basic contract and all Task Orders. Except as specified below, kickoff meeting requirements will be identified in individual Task Orders.

Within 15 business days following the contract award date, the contractor shall:

a) Conduct a Kickoff Meeting with the Government, which will cover requirements for the IDIQ contract, Task Order 0001, and Task Order 0002. The Kickoff Meeting shall be held at a contractor-provided facility in accordance with IDIQ PWS Section 5.1.1.1 to review goals and objectives, and to discuss technical requirements, administrative matters, security requirements, Government-Furnished Information/Materials/Equipment (GFI/GFM/GFE) (if any), schedule, review cycles, and invoicing

i. The Kickoff Meeting shall include, at a minimum, discussions on the following areas:
    a. Program Management
    b. Engineering
    c. Deployment
    d. Change Management
    e. Training
    f. Sustainment
    g. Testing
    h. Segment 2 (Operational Medicine)
    i. Cost and Budget

ii. All key personnel shall attend and participate in the Kickoff Meeting

b) Prepare a Meeting Agenda (CDRL A002) identifying specific topics of discussion and durations for the meeting. The agenda shall include at a minimum:
    i. contractor's organizational structure with named personnel
    ii. Integration Approach
    iii. Deployment Approach
    iv. Organizational Change Management and Training Approach
    v. Projected schedule with major milestones through Initial Operational Capability (IOC)
    vi. Tools to be used in execution of the contract

c) Conduct a Software Data Reporting (CSDR) meeting as a part of the IDIQ Contract and Task Orders 0001 and 0002 Kickoff Meeting
    i. Provide Presentation Materials (CDRL A003) to describe the approach to fulfilling contractual obligations with the Cost and Software Data Report (CSDR) (Attachment 6)

d) Prepare Presentation Materials (CDRL A003) based on the approved Meeting Agenda

e) Develop Meeting Minutes (CDRL A004)

f) Develop and submit draft versions of the following items for the Kickoff Meeting:
    i. An Integrated Program Management Report (IPMR) (CDRL A005)
    ii. A comprehensive Implementation Plan (CDRL A006) in accordance with the DHMSM DTCMP
    iii. A Contractor Master Test Plan (CMTP), a component of the Test Plan (CDRL A007), that details the contractor's testing approach consistent with the DHMSM Test Strategy

5.1.4 Product Demonstration

The contractor shall:

a) Provide EHR System demonstrations as requested by the Government. Product demonstrations may be at contractor or Government facilities

b) Demonstration shall include, but not be limited to:

   i. "To-Be" business and clinical workflows

   ii. EHR System role definitions

c) Provide EHR System functional and technical training to the DHMSM PMO staff

5.1.5 Reporting Requirements

The contractor shall:

a) Provide and maintain the:

   i. Monthly Progress Report (CDRL A008)

   ii. Competitive Subcontracts Report (CDRL A009) in accordance with FAR clause 52.219-9,

      a. Effectively implement their Government approved Small Business Subcontracting Plan throughout the life of the contract

      b. Provide for maximum practicable opportunity for Small Business to participate in contract performance consistent with efficient contract performance

      c. Meet all terms and conditions in the contract relating to Small Business participation. Inability to meet subcontracting goals may negatively affect a contractor's annual Government Contractor Performance Assessment Report (CPAR) rating

   iii. Contractor Work Breakdown Structure (CWBS) and CWBS Dictionary (CDRL A049), which are components of the IPMR (CDRL A005) and are needed for adequate management and control of the contractual effort, in accordance with the following:

      a. MIL-STD-881C, Department of Defense Standard: Work Breakdown Structures (WBSs) For Defense Materiel Items

      b. DoD 5000.04-M-1 Cost and Software Data Reporting (CSDR) Manual,

      c. EHR System solution Contractor Cost and Software Data Report (CSDR) Plan (Attachment 6)

b) Obtain Government approval prior to making any changes to the CWBS and CWBS Dictionary

c) Operate, maintain, and provide to the Government, with remote access, an electronic dashboard that includes an integrated status of the infrastructure, services, and events, incidents, and the associated impacts and mitigation plans. At a minimum, the dashboard should include:

   i. Continuous system monitoring information

   ii. All parameters listed in the IDIQ PWS tasks 5.2.9.e and 5.2.9.f

   iii. GAL integration status

iv. Site deployment status

v. Parameters gleaned from site visits

vi. Number of users to be trained and number users that have successfully completed training by site

vii. Competency Test Report and User Experience Satisfaction Survey results

d) Report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DoD via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil.

5.1.5.1 Cost Data Reporting

The contractor shall:

a) Comply with Contractor Cost Data Reporting (CCDR) guidance in accordance with the CSDR Plan (Attachment 6) and DoD 5000.04-M-1, Cost and Software Data Reporting Manual

b) Ensure CCDR requirements are flowed down to any lower tier contractor that has a contract value over $20 million or is designated by the Government as doing high risk, high value, or high technical interest work on the contract

c) Incorporate subcontractor CCDR data in its CCDR submission

d) Provide a Functional Cost Hour Report (CDRL A010), Cost Data Summary Report (CDSR) (CDRL A011), Software Resource Data Report (SRDR) (CDRL A012), and a Contractor Business Data Report (CDRL A047)

5.1.5.2 Earned Value Management

Earned Value Management requirements and applicability will be set forth in Task Orders.

When required, the contractor shall:

a) Establish, use, and maintain an Earned Value Management System (EVMS) that complies with DFARS 252.234-7001, 252.234-7002 and ANSI/EIA-748C

i. If applicable, ensure the EVMS requirements are flowed down to all subcontracts at all tiers

ii. The EVMS shall be formally validated and accepted by the Defense Contract Management Agency (DCMA)

iii. The EVMS shall be capable of the following:

a. Relate resource planning to schedules and technical performance requirements

b. Integrate technical performance, cost, schedule, and risk management

b) Provide a Contract Funds Status Report (CFSR) (CDRL A013)

c) Conduct an Integrated Baseline Review (IBR) no later than six months after each of the following, as applicable:
   i. Task Order issuance
   ii. Exercise of contract options
   iii. Incorporation of modifications

d) Prepare an Agenda (CDRL A002), Presentation Materials (CDRL A003), and Meeting Minutes (CDRL A004) in support of the IBR

e) Provide an IPMR (CDRL A005) which includes Formats 1-7 of the IPMR Data Item Description (DID) DI-MGMT-81861

5.1.6 Quality Management

QM reduces and eventually eliminates nonconformance to specifications, standards, and customer expectations in the most effective and efficient manner. The Government will monitor the contractor performance under this contract in accordance with the Task Order Quality Assurance Surveillance Plans (QASPs) (Attachments 17 and 18).

The contractor shall:

a) Have and maintain a Quality Management System (QMS) with processes that meet contract requirements and program objectives while ensuring customer satisfaction and defect-free products/processes. At a minimum, the contractor's QMS shall meet the following key criteria:
   i. Establish capable processes
   ii. Monitor and control critical product and process variations
   iii. Establish mechanisms for feedback of field product performance
   iv. Implement an effective root-cause analysis and corrective action system
   v. Establish procedures for continuous process improvement
   vi. Document and contain procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on the contractor's internal auditing system
   vii. Be made available to the Government for review

b) Continually improve the effectiveness of the QMS used to monitor contract performance

c) Ensure the requirements of this section (and subsection) are flowed down to all subcontracts at all tiers

5.1.6.1 Quality Control

Quality Control ensures that the services specified in this contract and Task Orders are delivered in accordance with the performance standards in the DHMSM QASP (Attachment 14). These performance standards prescribe acceptable levels of timeliness and quality for the services to be delivered. The contractor's Quality Control Plan will establish methodologies by which the contractor will meet or exceed program schedule, quality, and performance requirements set forth in each Task Order.

The contractor shall:

a) Develop a single Quality Control Plan (QCP) (CDRL A014) that aligns to the DHMSM Quality Assurance Surveillance Plan (QASP) (Attachment 14)

b) Continually assess the state of compliance of the DHMSM services with the schedule, quality, and performance requirements

c) Take proactive steps to determine and implement improvements to the level of services delivered

d) Provide personnel, tools, and processes to monitor, manage, and regulate performance and security and continuously optimize performance

e) Generate an incident ticket when the EHR system operates below a satisfactory standard as defined in the QASP

f) Provide a summary of DHMSM performance standards as part of the Monthly Progress Report (CDRL A008) and include recommendations to improve DHMSM EHR System performance

g) Provide the Government access to tools, data stores, and reporting scripts to verify, validate, and audit performance management information

5.1.7 Risk Management

Risk Management provides an organized means of identifying, measuring, ranking risks and developing, selecting, and managing options for resolving or mitigating risks.

The contractor shall:

a) Develop and implement a Risk Management Program consistent with the PEO Risk Management Plan

b) Develop and submit a comprehensive Contractor Risk Management Plan (CRMP) (CDRL A015)

c) Perform an initial Risk Assessment and report the findings in the Risk Assessment Report (CDRL A016)

d) Continuously perform risk assessments and report findings in the Monthly Progress Report (CDRL A008) and at PMRs, technical reviews, program milestones and configuration audits in Presentation Materials (CDRL A003)

e) Identify and utilize a Risk Management tool to manage risk information and compile a comprehensive program risk register and provide Government access as requested

5.1.8 Schedule Management

The contractor shall:

a) Develop and maintain an Integrated Master Plan (IMP) (CDRL A017) and a Contractor Integrated Master Schedule (CIMS) that aligns with the CWBS (CDRL A049) and submit as part of the Integrated Program Management Report (IPMR) (CDRL A005).

   i. Updates to the IMP (CDRL A017) will be made to incorporate programmatic changes as approved by the Government

   ii. All schedules required throughout the contract must be contained in the CIMS

b) Perform analysis of the CIMS, report in the Monthly Progress Report (CDRL A008) any existing or potential problem areas, and recommended corrective actions required to minimize or eliminate negative impacts to the schedule

c) Maintain and update the CIMS to reflect the status of or any changes to the contractor's detailed activities

d) Obtain Government approval prior to making any changes to the CIMS

5.1.9 Management of Government Property

The Government may provide hardware and/or software in support of a specific Task Order. Such Government-Furnished Property (GFP) will be specified in the individual Task Orders.

GFP provided to the contractor in support of individual Task Orders shall be tracked through applicable procedures provided by the PCO in accordance with the FAR. Property shall be accounted for and marked for identification and tracking purposes with the Contract Number, Task Order Number, Serial Number and other information as required by the PCO.

All GFP shall be returned to the Government at the completion of each Task Order unless otherwise specified. The Government may provide information (e.g., technical data, applicable documents, plans, regulations, specifications, etc.) in support of a specific Task Order.

The contractor shall:

a) Operate in Government provided workspace on an as-available basis while on trips to Government facilities or installations. Such Government-furnished workspace will be specified in individual Task Orders

b) Mark and report all assets procured for the Government in accordance with the below sub-paragraphs. Affix Item Unique Identifier (IUID) tags to all new assets prior to shipment for Government receipt

   i. Defense Federal Acquisition Regulation Supplement (DFARS) Clauses 252.211-7003 and 252.211-7007

   ii. DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property

   iii. MIL-STD-130N, DoD Standard Practice Identification Marking of US Military Property

c) If any GFP is provided or Contractor-Acquired-Government Owned Property (CAP) acquired, the contractor shall affix IUID tags

d) Perform physical asset audits in accordance with DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property

   i. Perform physical asset audits at a minimum of every three years. Sampling methods may be used where appropriate, provided they achieve statistically valid results. Sampling methods may not be used for classified or sensitive property

   ii. Report audit results in the Asset Audit Report (CDRL A018)

   iii. A 98% physical accuracy rate for property must be achieved and maintained

e) Develop and maintain an enterprise inventory accounting system which specifies, at a minimum:

i. Product description
ii. Make, model/part number
iii. Government tag number
iv. Date of receipt
v. Name of recipient
vi. Location of receipt
vii. Current location
viii. Purchase cost (if Contractor-Acquired, Government-Owned Property (CAP))
ix. Contract/order number under which the equipment is being used

f) Make the enterprise inventory accounting system available for Government review within one business day of Government request

5.1.10 Security Management

Any classified work performed under this contract will be specified in the DD-254 (Attachment 7). Appropriate security clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted. All security-related requirements shall be flowed down to all subcontractors at all tiers. The contractor shall have a SECRET facility clearance (FCL) at the time of Contract Award.

5.1.10.1 Security Officer

The contractor shall designate a Security Officer to support those contractor personnel requiring access to government facility/installation and/or access to information technology systems under this contract. The Security Officer shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on contract. Responsibilities include entering and updating the personnel security related and mandatory training information within the Monthly Progress Report (CDRL A008).

5.1.10.2 Personnel

The contractor shall:

a) Conform to the security provisions of DoD 5220.22M – National Industrial Security Program Operating Manual (NISPOM), DoD-8570.01-M/DoD-8140, and the Privacy Act of 1974

b) Ensure its personnel possess and can maintain security clearances at the appropriate level(s), and are certified/credentialed for the Cyber Security Workforce (CSWF), as applicable, prior to any labor hours being charged on contract

c) Validate, at a minimum, that the background information provided by its employees charged under this contract is correct, and the employee shall have attained at a minimum a determination that they meet the minimum standard for a Position of Trust with appropriate IT category access.

NOTE: If a final determination is made that an individual does not meet the minimum standard for a Position of Trust with appropriate IT category access after a National Agency Check with Law and Credit (NACLC) or Moderate-Risk Background Investigation (MBI), then the individual

shall be immediately and permanently removed from facilities, projects, and/or programs supporting the DHMSM Program. If an individual who has been submitted for a security clearance is "denied" for a clearance or receives an "Interim Declination", that individual shall be immediately removed from facilities, projects, and/or programs supporting the DHMSM Program until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task and contract.

5.1.10.3 Personnel Clearance

All personnel associated with this contract shall occupy a position of public trust and shall have completed an appropriate background investigation. Some of the individual Task Orders issued against this contract shall require personnel having higher clearance levels up to SECRET. These tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data and spaces as required and a need to know. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the DoD Central Adjudicative Facility (DoDCAF) and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as required by DoDI 8500.01, Cybersecurity and DoDI 8510.01, Risk Management Framework for DoD Information Technology. Any future revision to the respective directive and instruction shall be applied to the Task Order level as necessary. Contractor personnel shall handle and safeguard any unclassified but sensitive and classified information in accordance with appropriate Department of Defense security regulations. Any security violation shall be reported immediately to the PCO and Project Manager. Foreign national employees employed in their home countries shall meet equivalent host nation security requirements.

5.1.10.4 Access Control of Contractor Personnel

5.1.10.4.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

a) The majority of Government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD Manual 5220.22M (NISPOM) not later than two (2) weeks prior to visit – timeframes may vary at each facility/installation. For visitation to all other Government locations, visit request documentation shall be forwarded directly to the on-site facility/installation security office (to be identified at Task Order level) via approval by the COR

b) Depending on the facility/installation regulations, contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement

c) All contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location

5.1.10.4.2 Identification and Disclosure Requirements

As required in DFARS 211.106, contractors shall take all means necessary to not represent themselves as Government employees. Contractor-occupied Government facilities such as offices, separate rooms, or cubicles shall be clearly identified with contractor-supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

All contractor personnel shall:

a) Be clearly identifiable while on Government property by wearing appropriate badges

b) Identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract

5.1.10.4.3 Government Badge Requirements

As specified in FAR clause 52.204-9, some contract personnel shall require a Government issued picture badge. While on Government installations/facilities, contractors shall abide by each site's security badge requirements. Various Government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel as required. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF85P for CAC card) to the applicable Government security office via the contract COR. The contractor's appointed Security Officer, which is required in FAR clause 52.204-9, shall track all personnel holding local Government badges at contract or Task Order level.

5.1.10.4.4 Common Access Card (CAC) Requirements

Some Government facilities/installations require contractor personnel to have a Common Access Card (CAC) for physical access to the facilities or installations. Contractors supporting work that requires access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

a) In accordance with Directive-Type Memorandum (DTM-08-003), issuance of a CAC will be based on the following four criteria:

   i. Eligibility for a CAC – to be eligible for a CAC, contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the government on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification

   ii. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Contractor Verification System (CVS)

iii. Completion of background vetting requirements according to FIPS PUB 201-1 and DoD Regulation 5200.2-R – at a minimum, the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a NACLC to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Personnel requiring a CAC under Defense Health Agency (DHA) shall contact the appropriate authority to obtain the latest requirements and procedures

iv. Verification of a claimed identity – all personnel will present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS

b) When the contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC shall have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request (SAAR) form to the contract's specified COR. In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, the contractor shall seek latest guidance from its appointed company Security Officer and the DHA Security office:

i. For annual DoD Cybersecurity Awareness training, contractors shall use this site: http://iase.disa.mil/index2.html. For those contractor employees requiring initial training and do not have a CAC, contact the DHA Security office for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html

ii. For SAAR form, the contractor shall use DD Form 2875 (August 2009). Contractors can obtain a form from the website: https://navalforms.documentservices.dla.mil/.

5.1.10.4.5 Personnel Check-in and Check-out Procedures

All DHMSM contractor personnel requiring or possessing a government badge and/or CAC for facility and/or IT access shall be in compliance with the most current revision of Check-in and Check-out Procedures for contractors applicable to the facility in accordance with DHA security policy. At contract award and throughout contract completion, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this contract within the required timeframe as cited in the Check-in and Check-out instructions. As required, contractor employees shall complete and route the most current revision of the Check-in list or Check-out list as applicable. The contractor's Security Officer shall ensure all contractor employees whose services are no longer required on contract return all applicable Government documents, badges, and GFP to the Government.

5.1.10.5 IT Position Categories

In accordance with DoDI 8500.2 and DoD 8570.01-M a designator shall be assigned to certain contractor employees that indicate the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, the IT Position categories include:

a) IT-I (Privileged)

b) IT-II (Limited Privileged)

c) IT-III (Non-Privileged)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The contractor Program Manager shall assist the COR or other designated Government official in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication shall be performed in accordance with DoDI 8500.2. IT Position Categories shall be determined based on the following criteria:

5.1.10.5.1 IT-I Level (Privileged)

Positions in which the contractor is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated SSBI or SSBI-PR. The SSBI or SSBI-PR shall be updated a minimum of every five (5) years.

5.1.10.5.2 IT-II Level (Limited Privileged)

Positions in which the contractor is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed at the IT-II Position level by a higher authority to ensure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated NAC.

5.1.10.5.3 IT-III Level (Non-privileged)

All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated NAC.

5.1.10.6 Security Training

Regardless of the contract security level required, the contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the contractor's designated Security Officer shall track the following information: security clearance information, Common Access Cards issuance and expiration dates, cybersecurity training, Privacy Act training, and Cyber Security Workforce (CSWF) certifications,

etc. The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22M.

5.1.10.7 Operations Security (OPSEC) Requirements

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. The contractor, including subcontractors if applicable, shall perform OPSEC as directed in DoDD 5205.02E.

5.1.10.8 OPSEC Training

The contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. OPSEC training may be provided by the Government or the contractor and shall, as a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the contract/Task Order, and review OPSEC requirements if working at a Government facility. OPSEC training requirements are applicable for all contractor personnel during their entire term supporting this contract. Any EHR System training materials developed by the contractor shall be reviewed by the DHA Security Officer, who will ensure it is consistent with DHA OPSEC policies.

5.1.10.9 Classified Contracts

Any OPSEC requirements identified for a classified portion of this contract will be specified in the DD Form 254 (Attachment 7).

5.1.10.10 Data Handling

At a minimum, the contractor shall handle all data received or generated under this contract at level that is commensurate with For Official Use Only (FOUO) material. Specific or additional data handling requirements may be provided in individual Task Orders. Any classified information received or generated shall be handled in accordance with the attached DD Form 254 (Attachment 7) and shall be in compliance with all applicable PWS references and to other applicable Government regulations, instructions, directives, policies, and procedures.

5.1.10.11 Records Management

When creating and maintaining official Government records, the contractor shall:

a) Comply with all federal requirements established by 44 U.S.C. Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management

b) Comply with DoD Administrative Instruction No. 15 (DOD AI-15), “OSD Records and Information Management Program”

5.1.10.12 Business Associates Agreements (BAA)

The contractor shall conform to the following and shall submit the signed agreement located at: http://tricare.mil/tma/privacy/contractlanguage.aspx.

5.1.10.12.1 General Provisions

The contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business Associate Agreement (BAA) between the contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. This paragraph serves as the required BAA. As a Business Associate, the contractor shall comply with the HIPAA Rules and the DoD HIPAA Issuances applicable to a business associate performing under this Contract.

The following terms used, but not otherwise defined in this section, shall have the same meaning as those terms have in the DoD HIPAA Issuances: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information (Unsecured PHI), and Use.

5.1.10.12.2 Contractor Responsibilities

The contractor shall:

a) Not use or further disclose PHI other than as permitted or required by the Contract or as Required by Law

b) Use appropriate safeguards, and comply with the HIPAA Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Contract

c) Report to DHA any breach of which it becomes aware, and shall proceed with breach response steps as required by section 5.1.10.18

   i. With respect to electronic PHI, respond to any security incident of which it becomes aware in accordance with any cybersecurity provisions of this Contract

   ii. immediately initiate breach response as required by paragraph 9, if at any point the contractor becomes aware that a security incident involves a breach

d) In accordance with 45 CFR 164.502(e)(1)(ii)) and 164.308(b)(2), respectively, as applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the contractor agree to the same restrictions, conditions, and requirements that apply to the contractor with respect to such PHI

e) With respect to individual rights of access to PHI, make available PHI in a designated record set to the individual or the individual's designee as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.524

   i. If the contractor intends to deny the individual's request, forward it (within seven working days of receipt) to the CO. The CO shall make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The CO shall notify the individual, with a copy to the contractor, of any approved or denied access determinations and the reason for any denial. The individual may appeal the denial determination to the DHA Privacy Office

f) Make any amendment(s) to PHI in a designated record set as directed or agreed to by DHA, or take other measures as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.526

g) Maintain and make available to the Government the information required to provide an accounting of disclosures to the MHS or to the individual as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.528

h) Comply with the requirements of the HIPAA Rules to the extent the contractor is to carry out one or more of DHA's obligation(s) under the HIPAA Rules

i) Make its internal practices, books, and records available to the HHS Secretary for purposes of determining compliance with the HIPAA Rules

5.1.10.12.3 General Use and Disclosure Provisions

The contractor may only use or disclose PHI as necessary to perform the services set forth in this Contract or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA Issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by the Contract or directed by DHA. The contractor agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances. The contractor shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances or HIPAA Privacy Rules if done by the covered entity, except uses and disclosures for the contractor's own management and administration and legal responsibilities or for data aggregation services as set forth below in subsection 5.1.10.12.4.

5.1.10.12.4 Specific Use and Disclosure Provisions

Except as otherwise limited in this section, the contractor may:

a) Use PHI for the proper management and administration of the contractor or to carry out the legal responsibilities of the contractor. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph

b) Disclose PHI for the proper management and administration of the contractor or to carry out the legal responsibilities of the contractor, provided that disclosures are required by law, or the contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the contractor of any instances of which it is aware in which the confidentiality of the information has been breached

c) Use PHI to provide Data Aggregation services relating to DHA's health care operations

5.1.10.12.5 Contractor Compliance with DHA Notices and Restrictions

DHA will provide the contractor with the notice of privacy practices that DHA produces in accordance with the DoD HIPAA Issuances and the corresponding 45 CFR 164.520. Upon notification by DHA of any changes in, or revocation of, permission by an individual to use or disclose his or her PHI, the contractor shall comply to the extent that such changes may affect the contractor's use or disclosure of PHI.

The contractor shall:

a) Upon notification by DHA, comply with any restriction on the use or disclosure of PHI that the Government has agreed to or is required to abide by under the DoD HIPAA Issuances or the corresponding 45 CFR 164.522 , to the extent that such restriction may affect contractor's use or disclosure of PHI

5.1.10.12.6 Permissible Requests by DHA

The Government will not request the contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules or any applicable Government regulations (including without limitation, DoD HIPAA Issuances) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the contractor as otherwise permitted by this Contract.

5.1.10.13 Freedom of Information Act (FOIA)

The contractor shall:

a) Comply with the following procedures if it receives a FOIA request and immediately contact the DHA FOIA Officer for evaluation/action

   i. Forward the request immediately to the DHA FOIA Officer and the DHMSM PCO

   ii. Direct contact, including interim replies, between contractors and such requestors is not authorized

5.1.10.14 Systems of Record

The contractor shall:

a) Identify to the PCO systems of records that are or will be maintained or operated for DHA where records of PII collected from individuals are maintained and specifically retrieved using a personal identifier

b) Coordinate with the DHA Privacy Office to complete systems of records notices (SORNs) for submission and publication in the Federal Register as coordinated by the Defense Privacy and Civil Liberties Office, and as required by the DoD Privacy Act Issuances

c) Comply with the additional systems of records and SORN guidance, in coordination with the DHA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by the DoD Privacy Act Issuances, Office of Management and Budget (OMB) Memorandum 99-05, Attachment B, and OMB Circular A-130

d) Promptly advise the DHA Privacy Office of changes in systems of records or their use that may require a change in the SORN

5.1.10.15 Privacy Impact Assessment (PIA)

The contractor shall:

a) Provide for the completion of a PIA for any applicable systems that collect, maintain, use or disseminate PII or PHI about members of the public, federal personnel, contractors, or in some cases foreign nationals

b) Establish practices that satisfy the requirements of DoDI 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance.”

c) Send completed DD Form 2930s to the DHA Privacy Office for review and approval, with a copy to the PCO

Use the DHA PIA Guide and DoD-Approved PIA Template to complete the DD Form 2930

5.1.10.16 Data Sharing Agreement

The contractor shall:

a) Consult with the DHA Privacy Office to determine if the contractor must obtain a Data Sharing Agreement (DSA) or Data Use Agreement (DUA), when MHS data that is managed by DHA will be accessed, used, disclosed or stored, to perform the requirements of this Contract

b) Comply with requests for additional documentation by the DHA Privacy Board when requesting PHI for research

c) Comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and the DoD HIPAA Issuances. Comply with the DoD Privacy Act Issuances

d) Submit a Data Sharing Agreement Application (DSAA) to the DHA Privacy Office

    i. If the application is approved, the requestor shall enter into one of the following agreements, depending on the data involved:

        a. DSA for De-Identified Data

        b. DSA for PHI

        c. DSA for PII Without PHI

        d. Data Use Agreement for Limited Data Set

    ii. DSAs are active for one year, or until the end of the current option year, whichever comes first

    iii. Provide a Certificate of Data Disposition (CDD) to the DHA Privacy Office, if the DSA will not be renewed.

5.1.10.17 Privacy Act and HIPAA Training

The contractor shall:

a) Ensure that all of its employees, including subcontractors and consultants that perform work on this Contract, complete training on the Privacy Act, HIPAA, the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act, 42 U.S.C. 290dd-2, and the ADAMHA implementing regulations, 42 CFR Part 2, within 30 days of being assigned to this Contract and on an annual basis thereafter. Completion of this training shall be documented in a certificate

b) Maintain all certificates of training and provide to the Government upon request

5.1.10.18 Breach Response

Department of Defense (DoD) 5400.11-R, "DoD Privacy Program," defines a breach as the “actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected.”

45 CFR 164.402, used by HHS, defines a breach as the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of 45 CFR 164.402 which compromises the security or privacy of the protected health information.

Breaches are not to be confused with security incidents (often referred to as cyber security incidents when electronic information is involved), which may or may not involve a breach of PII/PHI. The DHA Privacy Office will determine the type of breach.

The contractor shall:

a) Report all breaches to the Government, assess the breach incident, notify affected individuals, and take mitigation actions as applicable

   i. If a breach involves only PII, then comply with DoD Privacy Act Issuance breach response requirements only

   ii. If a breach involves non-HHS PHI (a subset of PII), then comply with DoD Privacy Act Issuance breach response requirements only

   iii. If a breach involves HHS PHI, then comply with both the DoD Privacy Act Issuance breach response and HIPAA Breach Rule

b) Follow applicable DoD cybersecurity requirements under its contract in the event of a security incident not involving a PII/PHI breach

c) Follow any required cyber security incident response procedures to the extent needed to address security issues, as determined by DoD/DHA

5.1.10.18.1 Reporting Provisions

The contractor shall:

a) Report the breach within one hour of discovery to the US Computer Emergency Readiness Team (US CERT), and, within 24 hours of discovery, to the DHA Privacy Office and the other parties, as set forth below

   i. The contractor is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the contractor

   ii. If multiple beneficiaries are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstance

   iii. Inform the DHA Privacy Office as soon as possible if it believes that “single event” breach response is appropriate; the DHA Privacy Office will determine how the contractor shall proceed and, if appropriate, consolidate separately reported breaches for purposes of contractor report updates, beneficiary notification, and mitigation

   iv. In the event the contractor is uncertain on how to apply the above requirements, the contractor shall consult with the PCO, who will consult with the Privacy Office as appropriate when determinations on applying the above requirements are needed

b) Submit the US-CERT report using the online form at https://forms.us-cert.gov/report/.

   i. Save a copy of the on-line report before submission to US-CERT

   ii. Record the US-CERT Reporting Number after submission

   iii. Submit the US-CERT report by the deadline

a. Although only limited information about the breach may be available as of the one hour deadline for submission

c) E-mail updated information as it is obtained, following the instructions at http://www.us-cert.gov/pgp/email.html

d) Provide a copy of the initial or updated US-CERT report to the DHA Privacy Office and the applicable Service-Level Privacy Office, if requested by either

i. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office

ii. Submit the contractor report to DHA within 24 hours by completing the New Breach Reporting Form DD 2959 at the Breach Response page on the DHA Privacy Office web site and emailing that form to the DHA Privacy Office, the DHA CO and COR, and the DHA Program Office (or Service-Level Privacy Office) applicable to the Contractor

iii. For the applicable Program Office, e-mail the notice to its usual Point of Contact (POC) unless the POC specifies another addressee for breach reporting. Encryption is not required, because Breach Report Forms should not contain PII/PHI. The email address for notices to the DHA Privacy Office is provided at the Privacy Office website breach response page

a. If electronic mail is not available, telephone notification is also acceptable, but all notifications and reports delivered telephonically must be confirmed by email as soon as technically feasible.

e) Submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions in red text when a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update

i. Examples of updated information include, but are not limited to: confirmation on the exact data elements compromised, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, follow-up, etc.

f) Submit report updates promptly after the new information becomes available

g) Provide updates to the same parties as required for the initial Breach Report Form

5.1.10.18.2 Individual Notification Provisions

If the Privacy Office determines that individual notification is required, the contractor shall:

a) Provide written notification to individuals affected by the breach as soon as possible, but no later than ten (10) working days after the breach is discovered and the identities of the individuals are ascertained

i. The ten (10) day period begins when the contractor is able to determine the identities (including addresses) of the individuals whose records were impacted

b) Submit the proposed notification to the parties to which reports are submitted under paragraph 5.1.10.18.1 for their review, and for approval by the DHA Privacy Office

c) Provide the DHA Privacy Office with the final text of the notification letter sent to the affected individuals upon request by the Government

d) Provide the text of the letter for each group if different groups of affected individuals receive different notification letters

   i. Copies of further correspondence with affected individuals need not be provided unless requested by the Privacy Office

   ii. PII shall not be included with the text of the letter(s) provided

   iii. The contractor's notification to the individuals, at a minimum, shall include the following:

      a. The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual that these data elements potentially have been breached

      b. The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so that the individual clearly understands how the breach occurred

      c. The individual(s) must be informed of what protective actions the contractor is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261

      d. The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) that the contractor may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information

e) Ensure any envelope containing written notifications to affected individuals is clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the contractor and/or subcontractor organization that suffered the breach

   i. The letter must also include contact information for a designated POC to include, phone number, email address, and postal address

f) Indicate in the initial or updated Breach Report Form if the contractor determines that it cannot readily identify, or will be unable to reach, some affected individuals within the 10 day period after discovering the breach

g) Within the 10 day period, provide the approved notification to those individuals who can be reached

   i. Other individuals must be notified within 10 days after their identities and addresses are ascertained

h) Consult with the DHA Privacy Office, which will determine the media notice most likely to reach the population not otherwise identified or reached

i) Issue a generalized media notice(s) to that population in accordance with Privacy Office approval

j) At no cost to the government, bear any costs associated with a breach of PII/PHI that the contractor has caused or is otherwise responsible for addressing

5.1.10.19 Effective Use of Controls

The contractor shall:

a) Screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government

b) Utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation

   i. This includes ensuring that provisions are in place that will safeguard all aspects of information operations pertaining to this contract in compliance with all applicable PWS references

   ii. Compliance with DoD Data-at-Rest security protocols is required on all portable electronic devices including storage of all types

   iii. Encryption/digital signing of communications is required for authentication and non-repudiation

5.1.11 Transition Planning

The contractor shall:

a) Develop a Phase-Out Transition Plan (CDRL A019) that identifies the services necessary to transition either all or a part of the services under this contract as directed by the Government. These services will be separately ordered as a standalone Task Order

b) Execute transition activities to ensure continuity of services, minimize any decreases in productivity, prevent degradation of services, and prevent negative impacts to the continuity of care during the transition period

c) Provide knowledge transfer, support successor job shadowing, training, and other activities in order to successfully transition operation of services

d) Transfer software licenses to the Government in accordance with clause H-2

e) Deliver all training documentation requested by the Government

f) Transfer documents, badges, CACs, and GFP to the Government

g) Identify and transfer or destroy any classified materials or information in accordance with the Government Security Officer's instructions

h) Deliver all technical data (TD), computer software (CS), and computer software documentation (CSD) generated in the performance of this contract pursuant to DFARS 252.227-7027. Additionally, deliver all commercial and non-commercial TD, CS, and CSD not generated in performance of this contract that is necessary, as determined by

the Government at its sole discretion, to operate and sustain the EHR system throughout its lifecycle

i) If requested by the Government, export and deliver all data content with context (e.g., schemas, data format, data descriptions, and metadata) in a Government approved common standard electronic machine-readable format

5.2 Enterprise Electronic Health Record (EHR) System

The contractor shall provide an EHR System (integrated inpatient/outpatient Best of Suite (BoS) solution, augmented by Best of Breed (BoB) products) that meets or exceeds all requirements in the Government RTM (Attachment 2).

The EHR System shall:

a) Meet or exceed all requirements in the Government RTM (Attachment 2) through configuration with minimal development and maximum utilization of existing infrastructure resources

b) Be capable of meeting any capability in the approved CONOPS that may not be expressly incorporated in the Government RTM (Attachment 2)

c) Integrate and present data from multiple disciplines (e.g. Radiology, Immunization, Lab) in a single view that allows access by both clinicians and patients

d) Provide access to a longitudinal medical record for each beneficiary that is globally available across all time zones (24/7/365) and across the full range of military operations

e) Minimize the distributed systems (onsite) footprint required to support the Enterprise EHR System while meeting all requirements in the Government RTM (Attachment 2)

f) Leverage existing hosting and network infrastructure to the greatest extent possible (not including new hardware related specifically to the EHR System application) while meeting all requirements in the Government RTM (Attachment 2)

g) Centralize enterprise functions into common government approved hosting environments (e.g., data warehouse, user web portal, business interfaces) to minimize cost, complexity and gain economies of scale while meeting all requirements in the Government RTM (Attachment 2)

h) Utilize Medical Community of Interest (Med-COI) network and security services to the greatest extent possible consistent with the DHMSM Data Communications Network and Enterprise Services Infrastructure Framework

i) Utilize Government-provided Tier 1 enterprise datacenter hosting and network services (i.e. Government DISA DECCs or Federal Risk and Authorization Management Program (FedRAMP) approved facilities) as described in the DHMSM Data Communications Network and Enterprise Services Infrastructure Framework

j) Provide interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability in compliance with DoD Instruction “Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense” (DODI 8320.02)

k) Support global deployment and implementation of all requirements for all users and beneficiaries associated with Segment 1 and Segment 2 facilities and environments

i. The Government RTM identifies the Government's best estimates of user demand for the EHR system. The EHR system shall be capable of accommodating and scaling to meet increased user demand beyond that in the Government RTM to meet DoD mission requirements (e.g., large-scale activation of the National Guard in response to a national disaster.) The contractor understands and agrees that any increase in user demand beyond that identified in the Government RTM will not entitle the contractor to an equitable adjustment to, or constitute a Government breach of, this contract

l) Address functional and technical system performance challenges of remote, disconnected and disadvantaged users that may be limited by current and projected network and hosting infrastructure

m) Support software assurance principles as outlined in Paragraph 5.5.2.1

n) Utilize and provide open and standardized application program interfaces (APIs) enabling open access to the data and data model

o) Support clinical data exchange requirements with Department of Veterans Affairs and other external healthcare providers to enable the exchange of health data

p) Support Patient-Centered Medical Home (Team Based Care Model)

q) Provide the healthcare providers and patients with the latest advancements in technology in a timely manner with minimal disruption to enhance care

r) Ensure 100% compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and with the Privacy Act of 1974 as amended

s) Comply with the Health Information Technology for Economic and Clinical Health Act, Feb 17, 2009

t) Support compliance with nationally recognized Health Industry Standards to include HL7, NwHIN, LOINC, RxNorm, SNOMED, ICD-10, Office of the National Coordinator (ONC), and others as they evolve throughout the system development lifecycle

u) Enable compliance with the DOD Information Technology Standards Registry (DISR)

v) Employ a design that complies with applicable cybersecurity requirements based on Mission Assurance Category (MAC) level 2 and sensitivity level of the system, receiving an authorization to operate (ATO) from the Authorizing Official (AO)

w) Implement a cybersecurity strategy capable of continuous monitoring to evaluate the system compliancy throughout the period of performance of the contract

5.2.1 Open System Architecture

The EHR system shall adhere to the design and development principles outlined in the DoD Open System Architecture (OSA) Contract Guidebook for Program Mangers.

The contractor shall:

a) Document their OSA design and development approaches including: component dependencies, interface design and management, technology insertion, and life cycle sustainability aspects via CDRLs described in Section 5.2.5

b) Include assessments of interoperability and plan for maintaining currency with ONC and national standards as appropriate in the System Subsystem Specification (SSS) (CDRL

A020), System Subsystem Design Description (SSDD) (CDRL A021), and Technology Refresh Plan (TRP) (CDRL A022)

c) Provide a data architecture (i.e., data format, metadata, schema, interfaces and tools) that adheres to standard data transport, semantics and syntax to support the exchange of medical records and administrative information from the EHR system to enable access to, and migration of, patient data without custom translation and transformation of proprietary data or the loss confidentiality, integrity or availability. If requested by the Government, export and deliver all data content with context (e.g., schemas, data format, data descriptions, and metadata) in a Government approved common standard electronic machine-readable format

d) Provide a TRP (CDRL A022) that minimizes obsolescence, promotes adoption of emerging standards and new technologies and maintains compliancy and currency with ONC and other applicable national standards through life cycle management and component modernization

e) Provide a modular design capable of being deployed (through a distributed, centralized, or a hybrid approach) to overcome infrastructure limitations to meet all requirements and performance standards in the Government RTM (Attachment 2) with minimal development

f) Provide well documented open application program interfaces and services (e.g., Libraries, SDKs, data access services) to facilitate integration with both standards-based and custom components (e.g., business systems, other clinical systems, internally developed applications, etc.)

g) Use system design and engineering processes (life-cycle support plan) that enable system improvements through upgrades of individual hardware, software modules, or interfaces with newer modular components without redesign of the entire system or large portions thereof (e.g., migration to a new thin client interface, adoption of integration technology standard such as FHIR) and without placing additional data rights/intellectual property rights constraints on the overall system design

5.2.2 Software Requirements

The contractor shall:

a) Provide all software licenses in accordance with Clause H-2 Enterprise Software Licensing and Software Maintenance and all clauses, identifications and assertions, terms, and conditions related to commercial and non-commercial technical data, computer software, and computer software documentation to support the configuration, integration, custom development, test, software management, training, deployment, and end-user usage of the EHR System

b) Provide non-commercial and Open Source Software (OSS) source code to support the configuration, integration, custom development, test, software management, training, deployment, and end-user usage of the EHR System for Segment 1 and Segment 2 via the Computer Software Products (CDRL A023)

c) Provide software configurations to support all Roles of Care (Role 1, 2, 3, and EnRoute installations) in accordance with Segment 2 Roles of Care and Descriptive Statistics (Attachment 13) and the Government RTM (Attachment 2)

i. Provide the EHR System Installation Guide (CDRL A036) to support the configuration of all Roles of Care

ii. Software configured for Operational Medicine (Roles of Care) must be capable of running on existing Operational Medicine minimum infrastructure indicated for that role of care in accordance with Segment 2 Roles of Care and Descriptive Statistics (Attachment 13) and the Government RTM (Attachment 2)

d) Document and present an overview of the contractor's Integrated Development Environment (IDE) as part of the Training Materials (CDRL A024) describing the tools processes and procedures used to configure and integrate the EHR System. The IDE description and training will prepare the Government for review, testing, and acceptance of the configuration and source code developed to accomplish EHR System requirements

e) Provide the Government user accounts and the means necessary to enable read access to the contractor's IDE (e.g., coding tools, build servers, code management and reporting systems, quality management system), located in the GAL(s), at any time, to independently validate development progress, assess quality, verify test status in support of SETRs and In-Process Technical Reviews throughout the EHR System Lifecycle

f) Provide access to all EHR system computer software to allow the Government to perform cybersecurity and software assurance scans of the computer software. This requirement applies to all EHR system computer software, including both source code and executable code, regardless of whether the EHR system computer software is specified as a deliverable under this contract. Support contractors under non-disclosure obligations with the Government, such as the Use and Non-Disclosure Agreement at DFARS 227.7103-7, may assist the Government with these cybersecurity and software assurance activities

g) Manage and track all software licenses required to establish, operate, and maintain the EHR System. Document the software license allocation and utilization in the Monthly Progress Report (CDRL A008)

h) Provide and update the DHMSM Enterprise Release Schedule inputs to the contractor Integrated Program Management Report (IPMR) (CDRL A005) to include:

i. SW release packages based on IAVM, and DHMSM security and system incidents as specified by the Incident Management Plan (CDRL A025)

ii. Planned Technology Refresh and Modernization activities documented in the TRP (CDRL A022)

iii. New installations and service upgrades

i) Identify and report issues and risk associated with software and report risks/issues and status of any mitigation actions in the Monthly Progress Report (CDRL A008) and at PMRs, technical reviews, program milestones and configuration audits in Presentation Materials (CDRL A002)

5.2.3 Hardware Requirements

The contractor shall:

a) Have the overall responsibility for compatibility design, procurement, implementation, and maintenance of all hardware and related material necessary to augment the existing infrastructure and deliver an operational EHR System that meets or exceeds the requirements specified in the Government RTM (Attachment 2), including Tier 2 and below in accordance with the DHMSM Data Communications Network and Enterprise Services Infrastructure Framework

b) Provide continual market analysis in accordance with the TRP (CDRL A022) to develop technological recommendations to improve existing hardware, peripherals, software, and processes in support of the EHR System where hardware is deployed (e.g., GALs, Test Data Center, DISA Data Centers, Training Centers, MTFs and MAAG Sites)

c) Ensure that hardware specifications fit into the overall DHMSM Data Communications Network and Enterprise Services Infrastructure Framework and comply with the DISA Approved Product List (Refer to CAC accessible DISA website https://aplits.disa.mil/processAPList.do)

d) Recommend a hardware design and specification for approval by the DHMSM PMO prior to purchasing hardware as specified by the SSDD (CDRL A021) (this excludes hardware existing in a contractor owned development or test facility)

e) Provide the comprehensive hardware architecture depiction, specifications, and key inputs into the SSDD (CDRL A021)

f) Deliver the hardware Asset Audit Report (CDRL A018) providing the configuration scripts/instructions and logical/physical hardware architecture for each deployed EHR System (e.g., GALs, Test Data Center, DISA Data Centers, MTFs and MAAG Sites)

g) Perform and maintain asset management for the Government including: product warranties, service agreements, and expiration of maintenance agreements as applicable

h) Identify and report issues and risk associated with hardware and report risks/issues and status of any mitigation actions in the Monthly Progress Report (CDRL A008) and at PMRs, technical reviews, program milestones and configuration audits in Presentation Materials (CDRL A003)

5.2.4 Engineering Site Visit and Analysis

The contractor shall travel to specified sites and conduct site visits to validate DoD/MHS environments and inform requirements analysis and design activities for the EHR System in accordance with the DHMSM Engineering Master Plan (EMP). Tasks at each site visit shall include, but are not limited to:

a) Perform the following assessments during the site visit to:

   i. Assess “As-Is” application, network and infrastructure architecture and performance as it applies to deploying and meeting the EHR System requirements specified in the Government RTM (Attachment 2)

   ii. Assess clinical workflows to correct, extend and derive use cases and data requirements required to configure and test system workflows

   iii. Assess the site’s medical devices and system interfaces against the provided list of DHMSM system and medical device interfaces specified in the Government RTM (Attachment 2)

iv. Assess communication and computing infrastructure impact to the contractor's proposed EHR System deployment design's ability to meet:

a. Government RTM (Attachment 2) requirements

b. QASP (Attachment 14) performance standards

c. DHMSM Interface Strategy and PEO Data Management Strategy data synchronization capabilities

v. Validate site capacity and provide a Site Visit Report (CDRL A041) to update site-specific annotated drawings indicating planned and as-installed EHR System and allied support facilities required to support EHR System installation (e.g., HVAC, power, fire suppression and detection systems, electrical systems and power panels, etc.)

vi. Validate the site-specific MTF code and, if necessary, recommend an update to the site-specific MTF code component of the Site Visit Report (CDRL A041)

b) Conduct business process reengineering workflow analysis to establish "To-Be" models mapping EHR System workflows to reflect desired DoD functionality. Artifacts developed from this process will be documented using the DODAF standards and documented as specified in Business Process Workflow Diagrams and Role Definitions (CDRL A026)

c) Perform analysis to accurately describe and implement user workflows and identify means to assess improved efficiency and achieve meaningful use. This analysis includes:

i. Assess the current and future demands for clinical transactions and their impact to services and computing resources as well as future plans for workload growth

ii. Incorporate capacity and demand engineering services into the SSS (CDRL A020) requirements and design activities of new and modified services

iii. Analyze measurement data to include the impact of new releases on the EHR's ability to meet user population, transaction volumes and hardware/system capacity

d) Conduct gap analysis of site assessment data to identify system requirements, the deployment design impact on existing infrastructure, medical devices, interfaces, performance factors (i.e., total system users, transaction volumes), and clinical functions of the EHR System architecture. At a minimum, the following activities shall be conducted:

i. Analyze the installed network and hosting infrastructure to identify impact to proposed enterprise design and performance requirements and update specifications in SSS (CDRL A020)

ii. Analyze data flows, archiving, reporting, analytics, enterprise and site specific migration, data synchronization and use of data standards to define the system interfaces and data system requirements that are used to develop the SSDD (CDRL A021) and Contractor Data Management Plan (CDRL A027)

iii. Analyze site assessments to identify the impact of gaps to the contractor's System Architecture as defined in the SSDD (CDRL A021) for implementing the EHR System

iv. Provide an in process technical review with the DHMSM SE IPT to review the results of the gap analysis and recommendations for the approved list of device and system interfaces to be included in the SSS (CDRL A020) via the Contractor Requirements Traceability Matrix (CRTM) (CDRL A028)

e) Conduct performance analysis to:

i. Document and assess the current and future demands for services and computing resources as well as future plans for workload growth in the SSDD (CDRL A021) and TRP (CDRL A022)

ii. Document influences and projections on demand for computer and network resources as system requirements in the SSS (CDRL A020) and design criteria in the SSDD (CDRL A021)

iii. Incorporate capacity and demand engineering services into the requirements and design activities of new and modified services. Analyze measurement data to include the impact of new releases on capacity

f) Document the outcome of and the performance analysis in an SSS (CDRL A020). The SSS extends the Government RTM (Attachment 2) by capturing the detailed technical capabilities derived during analysis and design into requirements and specifications required to design, configure and integrate the EHR System capabilities. The CRTM (CDRL A028) shall provide traceability between SSS and the RTM. The CRTM (CDRL A028) shall also:

i. Capture additional requirements as may exist, such as, system quality factors, environmental factors, logistics, and the cybersecurity security controls required for successful accreditation of the system

ii. Synchronize with the SSDD (CDRL A021), which will provide the implementation details of the requirements

iii. Continuously capture newly derived requirements and clarification of significant changes due to site visits, development/configuration efforts and new functional requirements in accordance with the PEO Configuration Management Plan

5.2.5 System Design

The contractor shall perform design activities in accordance with the DHMSM EMP and align the activities in a manner that supports mature Enterprise Architecture, System Designs and OSA principals. The design activities shall also leverage the results of site visits and the performance of in-depth system analyses.

At a minimum, the contractor shall:

a) Document the baseline design and end-to-end design description in the SSDD (CDRL A021) to include:

i. System definition

ii. Subsystem component definitions

iii. Configuration items

iv. Interface descriptions

v. Integrated enterprise depiction (System Interface Description)

vi. System hardware description

vii. Mapping of design specifications to the Government RTM (Attachment 2) and Government-approved SSS (CDRL A020) in the CRTM (CDRL A028)

viii. Open System Architecture design description

b) Deliver a corresponding Interface Control Document (ICD) (CDRL A029) for each unique DHMSM interface to the component and subsystem specifications that define the component checkout and subsystem verification procedures

c) Maintain a list of medical devices compatible with the EHR System and make available to the Government upon request (CDRL A005)

d) Develop the EHR Technical Baseline Documents (CDRL A030) including, at a minimum, the Enterprise Architecture artifacts, detailed below. The electronic renditions of these artifacts will be crafted in a format that may be imported into the government's identified architectural repository and provide content consistent with the DoD Architecture Framework (DoDAF) Version 2.0

i. Systems Interface Description (SV-1)

ii. System Resource Flow Description (SV-2)

iii. Operational Resource Flow Matrix (OV-3)

iv. Operational Activity to System Function Traceability Matrix (OV-6c)

v. System Resource Flow Matrix (SV-6)

vi. System Event Trace Matrix (SV-10c)

vii. Database Design Description (DBDD) (CDRL A031)

viii. Interface Control Document(s) (ICD) (CDRL A029)

ix. System Subsystem Design Document (SSDD) (CDRL A021)

x. Technology Refresh Plan (TRP) (CDRL A022)

e) Update SSDD (CDRL A021), contractor-generated architectural artifacts, SSS (CDRL A020) and CRTM (A028) to reflect the necessary modifications identified by gap analysis to implement the EHR System based on design changes

f) Define and document how the proposed EHR system follows an open systems approach, uses modular design and standards-based interfaces, and widely-supported consensus-based standards in the SSDD (CDRL A021). Demonstrate compliance with the SSDD during all design reviews and include at a minimum:

i. An architecture description of how the EHR incorporates appropriate considerations for re-configurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability

ii. A description of how external information exchange requirements are implemented in a standard and open manner as part of this effort

iii. Define how the EHR architecture will continue to promote the use of an open architecture as well as adoption of other standards and requirements, tailored to meet its specific Service and Joint requirements

iv. Provide a Software Development Plan (SDP) (CDRL A032) in accordance with ISO/IEC 12207 IEEE Std. 12207-2008, Second edition 2008-02-01, “Systems and software engineering – Software life cycle processes” that describes how the software engineering and test processes enable the addition and upgrades of components with newer modular components without redesign of the entire or large portions of the system

v. Describe any module or component interfaces that will be delivered with rights more restrictive than Specially Negotiated License Rights (SNLR) consistent with K-11, K-13, H-3, and H-8. Describe how compatibility and extensibility is maintained to overcome the use of any proprietary components or interfaces

vi. Describe how the EHR design will minimize dependencies on other modules (loose coupling), as evidenced by simple, well defined interfaces and by the absence of implicit data sharing

vii. Describe how the EHR design will maximize software independence from the hardware and operating system to facilitate technology refresh and enhance portability

viii. Describe how interfaces between the layers are built to open standards or that the technical data describing the interfaces will be provided to the Government with rights no more restrictive than SNLR consistent with K-11, K-13, H-3 and H-8

ix. Describe how the system architecture will minimize inter-component dependencies that allow components to be decoupled and reused, where appropriate, across various DoD or Service programs and platforms

g) Develop interface design descriptions in the SSDD (CDRL A021) for each interface requirement type defined in the CRTM (CDRL A028) and the SSS (CDRL A020). Interface design descriptions should, at minimum include:

i. Data attributes, sequence flow, external system/workflow dependencies, security, performance requirements

ii. Approach to contractor unit, system, and integration testing, and test success criteria

iii. Identification of interface and data exchange standards between the component, module or system and the interconnectivity or underlying information exchange medium

h) Make interface designs available upon request

i) Deliver a hardware and software deployment design in the SSDD (CDRL A021) based on the current MHS network and computing infrastructure that meets the requirements specified in the Government RTM (Attachment 2). The design must:

i. Identify critical performance areas by component

ii. Provide the means by which the performance will be analyzed and verified throughout development, testing, and deployment

iii. Recommend improvements to address network capacity and reliability

j) Analyze application hardware architecture assessment to design a systems hardware solution capable of meeting reliability, performance and security requirements in the SSDD (CDRL A021). Hardware design analysis shall, at a minimum, address:

   i. Storage utilization trends and the recommended reallocation and reuse of storage

   ii. Data storage management tools and designs to optimize the use of these tools

   iii. Data storage management virtualization scheme to improve accessibility and availability

   iv. Approaches to availability and redundancy and recommend improvements

   v. Server virtualization architectures to address scalability, availability and maintenance

   vi. The capability to recover data in the event of a disaster (e.g., more efficient and accessible backups, enhancements to storage recovery tools, and reallocation of existing storage to support cloud based DR sites)

k) Develop performance models to identify hardware and software component areas critical to scaling the solution (e.g., network latency, application server load, and database performance) at the system and enterprise levels in the SSDD (CDRL A021)

   i. Identify performance activities (e.g., IPRs, prototyping and test events) to continually assess and mitigate critical scalability risks as part of contractor testing in the GALs and documented in the IMS

   ii. Establish and implement, in collaboration with the Government, a system and tools to electronically capture, model, and readily generate tailored reports on the capacity of and demand for services and systems

l) Develop and maintain engineering inputs to the CIMS in coordination with the DHMSM Systems Engineering IPT that support DHMSM Technical Work Group charters and provides technical in process reviews to monitor critical capability, security, data and integration deliveries in accordance with the Program Work Breakdown Structure (WBS) (Attachment 5)

m) Support the Government's joint Initial Design Review (IDR)/Final Requirements review (FRR) by demonstrating the solution's ability to meet IDR criteria in the DHMSM EMP and to:

   i. Trace to and provide tests to satisfy functional requirements and OV-6c business and clinical workflows

   ii. Provide SSS (CDRL A020) traceability and gap analysis via the CRTM (CDRL 028)

   iii. Address coverage and approach to verify each non-functional performance and reliability requirement in the Government RTM (Attachment 2)

   iv. Address all Government RTM (Attachment 2) data requirements and plans to implement those identified in *PEO Data Management Strategy*

   v. Meet interface and data requirements defined in the *DHMSM Interface Strategy, PEO Data Management Strategy,* and Government RTM (Attachment 2)

vi. Meet and validate all EHR System performance requirements in the Government RTM (Attachment 2) and SSS (CDRL A020)

vii. Provide any cybersecurity design artifacts that demonstrate the EHR System compliance with the DoD cybersecurity requirements, as defined in the Security Authorization Package (CDRL A033), to achieve an ATO

viii. Provide performance modeling and testing

ix. Identify and meet Enterprise Integration dependencies as defined by requirements defined in the Government RTM, guidance provided by the *DHMSM Interface Strategy* and system requirements derived or modified during gap analysis

x. Demonstrate compliance with OSA approach and constructs outlined in SSDD (CDRL A021)

xi. Deploy hardware and software architecture to meet the Government RTM (Attachment 2) requirements and meet DHMSM infrastructure objectives as defined in the *DHMSM Data Communications Network and Enterprise Services Infrastructure Framework*

xii. Provide continuous unit, system and integration test during Contractor Integration and Test (CIT)

xiii. Achieve Engineering development schedule milestones and execute to plan

xiv. Provide the EHR Technical Baseline Document (CDRL A030) to support the Government establishment of an Allocated System Baseline

xv. Provide configuration designs to support the Segment 2 Roles of Care and Descriptive Statistics (Attachment 13)

5.2.6 System Configuration & Integration

The contractor shall:

a) Develop, integrate, and configure all aspects of the EHR System to meet the requirements as specified in the Government RTM (Attachment 2) and SSS (CDRL A020) in accordance with the processes and procedures specified in the contractor SEMP (CDRL A034)

b) Provide all necessary designs and associated documentation; develop and test interfaces; identify, construct and implement data migration capabilities in accordance with the engineering procedures outlined in the SEMP (CDRL A034) and Contractor Configuration Management Implementation Plan (CCMIP) (CDRL A035)

5.2.6.1 Interface Development

The contractor shall:

a) Develop the appropriate interfaces as specified in the SSS (CDRL A020), in accordance with the design guidance provided by the SSDD (CDRL A021) and to the specification outlined in the appropriate ICD (CDRL A029)

b) Update interface designs descriptions in the SSDD (CDRL A021) and ICD (CDRL A029) to reflect any modification to data attributes, sequence flow, external system/workflow

dependencies, security, performance requirements and approach to unit/system/integration test

5.2.6.2 Configuration Development

The contractor shall:

a) Implement workflows and business rules, including any reference data required to support clinical operations

b) Test system-level workflows to establish baseline performance characteristics as measurements for integration tests

c) Coordinate with MTF site personnel and designated functional representatives to conduct In Process Reviews to assess workflows deemed critical for accuracy and usability

d) Coordinate with the appropriate Segment 2 functional representation to conduct In Process Reviews to assess workflows and configurations for the Roles of Care

5.2.6.3 Additional Development Activities

If any additional software development is required, the contractor shall perform the following activities:

a) Gain approval of custom development requirements through the DHMSM Change Management Board (CMB)

b) Update component, interface, data, security, performance, workflow and interface design dependencies in the SSDD (CDRL A021) to reflect implementation and configuration of custom Configuration Items (CIs)

c) Ensure compatibility with particular hardware and software within the existing processing environment

d) Maintain traceability of custom software design to meet the requirements specified in the Government RTM (Attachment 2) and SSS (CDRL A020)

e) Deliver any additional software, including source code and executable code, developed under this section via Computer Software Products (CDRL A023)

5.2.6.4 Contractor Unit and System Testing

The contractor shall:

a) Provide the Government with the Contractor Unit and System Test results required to continually assess development progress, quality and performance with special emphasis on areas of scalability, security and integration risk identified in the SSDD (CDRL A021)

b) Perform the following incremental unit, system, and integration testing in accordance with the processes outlined in the SDP (CDRL A032), SEMP (CDRL A034) and the CMTP, a component of the Test Plans (CDRL A007):

   i. Automate testing so that builds and tests are conducted daily as appropriate

   ii. Conduct contractor system integration and testing based upon subsystems that can be end-to-end tested against the SSS (CDRL A020)

iii. Conduct regular integration load, stress, and peak testing to assess end-to-end reliability, availability, scalability of production hardware, network, and software components against performance models defined in the SSDD (CDRL A021) and performance requirements in the SSS (CDRL A020)

a. The CMTP, a component of the Test Plans (CDRL A007), shall provide methodologies to understand the impact due to network latency, application server load, and database performance

iv. Ensure that unit, system and integration testing includes data integrity and accuracy components in accordance with SSS (CDRL A020) and Contractor Data Management Plan (CDRL A027)

v. Provide data to meet DT&E entrance criteria as specified by the contractor SEMP (CDRL A034) in accordance with the DHMSM EMP and CMTP, a component of the Test Plans (CDRL A007)

5.2.7 System Installation

5.2.7.1 GAL Installation

Refer to Section 5.6.2 of the IDIQ PWS for GAL installation requirements.

5.2.7.2 Enterprise Infrastructure & System Installation

The full enterprise deployment will occur in Waves as defined in the Implementation Plan (CDRL A006) and DHMSM DTCMP. IOC will lay the foundational components of the EHR System enterprise infrastructure; the Full Deployment Decision (FDD) will authorize deploying additional enterprise components to meet scalability and functional requirements.

The contractor shall perform Segment 1 and Segment 2 enterprise infrastructure and system installation activities to include:

a) Delivery of the EHR System Installation Guide (CDRL A036)

b) Deploy initial enterprise infrastructure to support EHR System at IOC sites

c) Expansion (i.e., ordering and deployment) of infrastructure in Waves necessary to scale the EHR enterprise capability to meet the Government RTM (Attachment 2) requirements and QASP performance standards through FD/FOC

d) Conduct enterprise data migration in accordance with the Government RTM (Attachment 2) and Contractor Data Management Plan (CDRL A027)

5.2.8 Continuity of Operations (COOP), Disaster Recovery (DR), and Business Continuity Planning Services

Disaster Recovery encompasses the policies and procedures to prepare for recovery of technology infrastructure and business operations critical to an organization after a natural or human-induced disaster to partially or completely restore services and critical functions within a predetermined time after a disaster or extended disruption.

The contractor shall:

a) Design, install, operate, and maintain COOP capabilities to enable plans for emergency response and supporting infrastructure (e.g., storage and backup operations, off-site storage) for post-disaster recovery (DR) of information systems

b) Develop, maintain, and update the Disaster Recovery Plan (DRP) (CDRL A037) for restoration of operations in the event of an incident or disaster

c) Develop system and network designs that enable business and network operations capable of surviving individual component failure

d) Provide input to the Government for making system degradation decisions in the event of a disaster or incident

e) Provide input to the Government After Action Reports (AAR) and lessons learned following exercises

f) Execute emergency failover COOP requirements

g) Support annual exercises of the DRP (CDRL A037)

h) Enable the DRP (CDRL A037) in the case of an incident or disaster

5.2.9 System Quality and Performance Measures

The contractor SSDD shall identify the hardware and software components that are critical to meeting the capability and performance measures/design considerations and requirements stated in the DHMSM EMP and Government RTM (Attachment 2). The design shall identify how each component impacts system security, stability and performance.

The contractor shall conduct analysis and design activities for system quality and performance to include:

a) Align to the requirements identified in the Government RTM (Attachment 2) through a functional allocation process defined in the SEMP (CDRL A034)

b) Work with the DHMSM PMO and user community to:

   i. Identify the EHR interfaces, workflows, and infrastructure necessary to configure the EHR System

   ii. Assess and validate the performance acceptance criteria for Segment 1 and Segment 2 defined in the Government RTM (Attachment 2)

   iii. Provide recommended changes to performance acceptance criteria for Government approval in a Technical Report (CDRL A038)

c) Execute the CMTP, a component of the Test Plans (CDRL A007), to address performance requirements identified in the Government RTM (Attachment 2)

   i. Identify design and test events in the CMTP and engineering events in the CIMS via the IPMR to mitigate critical scalability risks

   ii. Develop performance models as part of system design process to identify critical areas to scaling the solution at the system and enterprise levels

d) When necessary, conduct prototyping and integration performance activities to mitigate and continually assess scalability as part of CIT in the GALs

e) Deliver a Monthly Progress Report (CDRL A008) that details performance for each of the EHR System requirements listed in the Government RTM (Attachment 2) as they pertain to both Segment 1 and Segment 2, which includes but is not limited to, the criteria below:

i. Client/Front End/Middle Tier Application Responsiveness – Ability of client tier to accommodate user loads. Provides insight into the architecture ability to load balance processes, handle security, and accommodate state-user interaction

ii. Application Servers Performance – Central Processor Unit/Memory/Cache utilization vs. total number of processing events. Provides insight into the efficiency of business and application design and its ability to meet/sustain client and service requests

iii. Data Storage Throughput – Disk/Redundant Array of Independent Disks (RAID) response time from time of request from the application to delivery of the data packet (with/without network and backplane latency)

iv. Database Responsiveness – Time a database takes to process a query, retrieve, package, and send the data back to requesting operation, function, etc.

v. Service Responsiveness – Time required for a service to process a request and package the return payload.

vi. Application Heartbeat Performance

f) Provide reliability and availability trend analysis and supporting data in the Monthly Progress Report (CDRL A008) to summarize analysis of assigned systems and services against established thresholds through growth curves to show prediction, trending, and monitoring of system's failure rates, derived from available information and/or prior systems. Reliability growth curves and models will be used to plan and monitor capability reliability during the system development lifecycle

5.3 Change Management

The contractor shall:

a) Deliver an Implementation Plan (CDRL A006) that defines the contractor's plan for deployment, training, change management, and sustainment of the EHR System to the DoD Enterprise

b) Deliver the Command Executive Briefing (CDRL A003) in accordance with the DHMSM DTCMP that details, at a minimum, the following information:

i. Enterprise deployment strategy

ii. Change management approach

a. EHR System User Role definitions

iii. Training approach

iv. Sustainment and helpdesk support

c) Propose recommended change management activities for the most efficient and effective change management support of the EHR System in the Monthly Progress Report (CDRL A008)

i. Execute such activities upon Government approval and direction

5.3.1 Business Process Reengineering

The contractor shall:

a) Participate in the Business Process Reengineering (BPR) IPT and advise or present industry leading practices, processes and workflow

b) Conduct a comparative analysis between the EHR solution-inherent workflows and the "As-Is" organizational business processes identified in the DoD Architecture Framework (DoDAF) Operational Viewpoint OV-6c Event Trace Descriptions in support of the PWS tasks in section 5.2.4 and provide recommendations on process re-engineering, change management and product configuration

c) Provide Business Process Workflow Diagrams and Role Definitions (CDRL A026) that define business and clinical workflows and describe functionality, improved efficiency, how meaningful use has been achieved, and establish EHR System user role definitions

d) Provide a Role Assignment Identification Document (CDRL A042) that maps Segment 1 and Segment 2 user roles to EHR System roles

5.4 Training

The contractor shall:

a) Ensure end-users and trainers obtain the skill sets necessary to utilize the EHR System and incorporate it into their daily workflows

b) Develop a training plan, as documented in the Implementation Plan (CDRL A006), that is specific to the DoD healthcare environment and workflows and that will meet the QASP performance standards related to training

c) Develop and deliver comprehensive Training Materials (CDRL A024) specific to the DoD healthcare environment and workflows which support the following methods of training at a minimum:

   i. Instructor-led Training (Classroom)

   ii. Instructor-led Training (Virtual)

   iii. Computer-based training (CBT)

   iv. Over-the-shoulder Training

d) Validate adequacy of training facilities and resources to meet site training requirements (e.g. computers, printers, projectors, connectivity, etc.) and report this analysis in the Technical Report (CDRL A038)

e) Provide training facilities and/or resources, as directed by the Government, to complete training of all end users

f) Update the Training Materials (CDRL A024) to reflect the Business Process Workflow Diagrams and Role Definitions (CDRL A026) in preparation for training support and change management

   i. Training shall be role based and align to the Business Process Workflows

g) Provide training to Government testers and test participants (e.g. SMEs, typical end users) in support of Government-Approved Laboratories (GAL) activities

5.4.1 Virtual Training Environment

The contractor shall:

a) Install, integrate and maintain the Virtual Training Environment (VTE) and provide scenario-based training simulations with synthetic data

b) Provide access to the Virtual Training Environment (VTE) prior to the start of Developmental Test and Evaluation (DT&E) as identified in Section 5.6.4

c) Ensure that the VTE provides the following utilities/requirements:

   i. A non-production instance of the EHR system, configured to the greatest extent possible, in order to resemble the production environment

   ii. Accessible locally or via the internet using desktops, laptops, smart phones, and tablet devices (mobile devices running DoD-approved operating systems)

   iii. Hosted in a DoD-approved commercial or Government network

      a. Provide DoD training developers and engineers with full access to the contractor's training environment(s) and the ability to install the VTE on the Government's servers

   iv. Accessible from Government networks

   v. Scalable to support approximately 10,000 to 15,000 concurrent virtual users

   vi. Capable of hosting digital media (documents, video and CBT training) in a virtual environment

   vii. Support remote document collaboration to facilitate knowledge management and change management

   viii. Host, deliver and store all virtual training and training materials in the Virtual Training Environment

   ix. There is no requirement for the VTE to operate in low or no-communication environments

5.4.2 Learning Management System

The DoD Learning Management System (LMS) will be utilized to host, deliver and store all virtual training and training materials.

The contractor shall:

a) Assist with loading the CBT and EHR System Demo provided in the Training Materials (CDRL A024) and Training Schedule provided in the Implementation Plan (CDRL A006) into the Government-provided LMS, as directed

b) Assist the Government with migration of data from an interim Government-provided LMS capability to an Enterprise level Government-provided LMS capability, as directed

5.5 Systems Engineering

The contractor will apply systems engineering processes that are:

a) Appropriate to the implementation of Off-the-Shelf software to address the concerns, issues, and drivers when implementing an EHR System

b) Consistent with the streamlined engineering approach and technical reviews outlined in the DHMSM EMP

5.5.1 Engineering SETR, Milestone and Review Support

There are six (6) formal System Engineering Technical Reviews (SETR) planned and defined in the DHMSM EMP. The contractor will conduct an engineering kickoff meeting no later than 15 days after Task Order 0001 issuance (supplementary to the PM Kickoff meeting identified in Section 5.1.3.1 of this PWS) to discuss the contractor's understanding towards the execution of the reviews. The contractor shall finalize the details of the SETR events (except for the kickoff meeting) with the participants 30 days in advance of the date of the SETR events. During the Initial Design and Final Requirements Review (IDR/FRR), the contractor and the Government will establish additional technical In Process Reviews (IPRs) to continually assess, at a minimum, evolving interface designs, enterprise integration architecture, hardware deployment designs, and engineering risk activities addressing performance and security requirements. Additional IPRs will be established throughout the program life cycle as required to support DHMSM Technical Work Groups and risk mitigation activities identified by the Government.

The contractor shall:

a) Develop and provide the following CDRLs in draft form to the Government no later than 30 days after issuance of the Task Order:
    i. System Engineering Master Plan (SEMP) (CDRL A034)
    ii. Contractor Configuration Management Implementation Plan (CCMIP) (A035)
    iii. Draft System Subsystem Specification (SSS) (CDRL A020)

b) Develop and provide the following CDRLs in draft form to the Government no later than 60 days after issuance of the Task Order:
    i. Business Process Workflow Diagrams and Role Definitions (CDRL A026)
    ii. (updated) System Subsystem Specification (SSS) (CDRL A020)
    iii. Contractor Requirements Traceability Matrix (CRTM) (CDRL A028)
    iv. System Subsystem Design Description (SSDD) (CDRL A021)
    v. Contractor Data Management Plan (CDMP) (CDRL A027)
    vi. Technology Refresh Plan (TRP) (CDRL A022)
    vii. Security Authorization Package(s) (CDRL A033)
    viii. Software Development Plan (SDP) (CDRL A032)
    ix. Version Description Document (VDD) (CDRL A045)
    x. System Safety Plan (SSP) (CDRL A048)

c) Schedule and conduct a combined IDR/FRR meeting upon completion of the Government review of the documents listed above and no later than 90 days after issuance of the Task Order
    i. Government and the contractor shall review and the Government will assess the system design
    ii. This review is intended to allow the Government to verify that the system requirements are sufficiently addressed and to establish the allocated baseline

d) Complete the FDR/TRR no later than ten (10) months after Task Order award. This review shall provide the Government with the assurance that the EHR system is ready for Developmental Test and Evaluation (DT&E)

    i. Identify critical technical capabilities, provide risk mitigation strategies, and establish the Product Baseline during this meeting

5.5.2 Systems Engineering Processes

The contractor shall:

a) Execute systems engineering processes capable of supporting the entire system development lifecycle

b) Develop a SEMP (CDRL A034) to support the processes, technical reviews, deliverables and engineering guidelines outlined in the DHMSM EMP

c) Develop a SDP (CDRL A032) to define:

    i. The software engineering processes, including: test approach, build strategy, code management, monitoring and reporting processes used during development

    ii. The software development processes including development environment and tools utilized by the contractor's software engineering and QA teams

    iii. A description of the application build environment, where source code is stored, how code is organized, how it is shared among developers, and how it is deployed to the final system to facilitate validation of quality and performance assessments

d) Execute systems engineering processes and update the Government approved SEMP (CDRL A034) in coordination with the DHMSM Technical Work Groups and Integrated Product Teams (IPT)

e) Provide SME participation in the planning and execution of the DHMSM Technical Work Groups and IPT meetings in accordance with the Government approved SEMP (CDRL A034)

f) Prepare Presentation Materials (CDRL A003) detailing how the contractor has achieved the entrance and exit criteria for each System Engineering Technical Review (SETR) in accordance with the DHMSM EMP

g) Identify, maintain and manage a list of critical technical design, performance, security and integration risks in the contractor's Risk Management tool

    a. Review, mitigation and test strategies to monitor the effectiveness and delivery of the EHR System

h) Provide network planning and definition, and enable the EHR System management functions to provide network operations, collection of performance characteristics, incident reporting, and system configurations across the system development lifecycle

i) Provide software quality assurance by abiding by the principles, in paragraph 5.5.2.1 Software Code Quality Checking (SCQC)

j) Use tools compatible with the list of tools provided in the DHMSM EMP

5.5.2.1 Software Code Quality Checking (SCQC)

Software assurance is defined by Federal Law for the Department of Defense (DoD) as the level of confidence that software 1) functions as intended and 2) is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle. DHMSM implements software assurance through a process called Software Code Quality Checking (SCQC). SCQC is defined as a scan of the source code, executables and related artifacts to ensure that the system under development can continue with development and test, and can meet the stated performance, maintainability, and usability requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. SCQC encompasses the use of static code analysis, static security analysis, dynamic code analysis, dynamic security analysis and architecture analysis and is usually performed using automated tools.

The Government further defines the following terms:

- Static analysis is the analysis of computer software and related documentation that is performed without actually executing programs built from the software
- Static security analysis is the analysis of computer software that is performed without actually executing programs to detect and report weaknesses that can lead to security vulnerabilities
- Dynamic program analysis is the analysis of computer software and related documentation that is performed by executing programs built from that software on a real or virtual processor
- Dynamic security analysis is the analysis of computer software that is performed by executing programs to detect and report weaknesses that can lead to security vulnerabilities
- Architectural analysis may be supported by automated tools but is usually conducted by manual walk-through of documentation and visual inspection of the code

The contractor shall:

a) Develop secure, reliable, resilient, assured software that is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software

b) Maintain controls in the provision of supplies and services to the Government to minimize supply chain risk in accordance with DoDI 5200.44.

c) Perform the reviews and scans to prevent, correct, and mitigate defects and vulnerabilities. Although primarily focused on developed items, the principles of SCQC will be applied to all OTS products, open source code, and third party code

d) Utilize automated tools and supplemental manual review to support scanning and inspection of the software to identify, correct, and mitigate application quality problems that are likely to cause functional as well as technical disruption

e) Utilize automated tools and supplemental manual review to support scanning/inspection of software to identify and correct/mitigate all Category I and Category II software vulnerabilities as identified in the DISA Security Technical Implementation Guides (STIGs) located at http://iase.disa.mil/stigs/

f) Implement a secure coding practice that conforms to the standards and direction outlined in the Application Security and Development STIG at: http://iase.disa.mil/index2.html

g) Submit a Technical Report (CDRL A038) that identifies any residual vulnerability in the software under development in accordance with ISO/IEC 25010, or equivalent framework, with particular emphasis on Reliability, Performance Efficiency and Maintainability of the code

   i. Identify the vulnerabilities by both the associated STIG ID and Common Weakness Enumeration (CWE) ID

   ii. Identify the recommended corrective action, e.g., correct during the next development cycle, mitigate through compensating controls, etc.

   iii. Correct all newly discovered vulnerabilities within the following specific timeframes:

      a. Category I: As soon as possible but no more than five (5) days after vulnerability was discovered

      b. Category II: Within 90 days after vulnerability was discovered

h) Make available to the independent SCQC team, at a minimum, the following artifacts in their current state at the time of the inspection regardless of the method used:

   i. Source code for all Enterprise Software (as defined in H-2) and all design time libraries and licenses (static analysis). Enterprise Software on the Common Criteria Portal (www.commoncriteriaportal.org) is not required to be scanned.

   ii. Executable code and libraries (dynamic analysis)

   iii. Application configuration artifacts

   iv. System Design Documents (SDD)

   v. System Sub-System Specification (SSS)

   vi. System Sub-System Design Document (SSDD)

   vii. Security Authorization Package

   viii. System Security Authorization Agreement (SSAA)

   ix. Interface Control Document (ICD)

   x. Database Design Document (DBDD) Test cases (dynamic analysis)

   xi. Version Description Document (VDD)

5.5.2.2 System Performance Monitoring

The contractor shall:

a) Utilize EHR System performance metrics, requirements, and objectives defined in the Government RTM (Attachment 2) to establish performance acceptance unit, system and integration test methodologies

b) Work with the Test and Evaluation Teams to use Measures of Effectiveness (MOEs) defined in the DHMSM Test Strategy to test and verify the EHR meets the Critical Operational Issues (COIs) for each of the domains of evaluation; MOEs may be

supplemented with other Measures of Performance (MOPs) for the sake of complete evaluation analysis

c) Develop specific test methodologies to assess the functional and technical system performance challenges required to support remote, disconnected and disadvantaged users that may be subject to limitations within current network and hosting infrastructure. The test shall verify that EHR System design in the SSDD (CDRL A021) addresses performance latency (points where the performance or capacity of the EHR system is limited by a single or limited number of components or resources) for these environments

5.5.3 Requirements Management

The contractor shall be responsible for requirements management from contract award throughout the system development lifecycle.

The contractor shall:

a) Document the contractor Requirements Management Process in the SEMP (CDRL A034) that integrates and aligns with the PEO Requirements Management Plan

b) Execute requirements management processes in accordance with established change control process defined in the CCMIP (CDRL A035) and the Implementation Plan (CDRL A006) and consistent with the PEO Configuration Management Plan and the DHMSM EMP

c) Provide a CRTM (CDRL A028) to maintain traceability between the Government RTM (Attachment 2), SSDD (CDRL A021), and SSS (CDRL A020)

d) Utilize the CRTM (CDRL A028) to trace and validate the approved requirements to the design specifications and approved test cases

e) Support the Engineering Change Request (ECR) process with high level impact analysis and potential recommendations that will require Government approval

f) Utilize a requirements management tool compatible with that of the Government to:

    i. Manage CRTM (CDRL A028) and EHR System requirements in accordance with the PEO Configuration Management Plan

    ii. Submit deliverables, inputs, and findings from baseline requirements analysis

g) Participate in weekly and monthly requirements team meetings

    i. Participation may involve presenting an ECR for review, presenting the mapping of requirements to the EHR System, and discussing overall requirements traceability

5.5.4 Configuration Management

Configuration Management (CM), when applied across the EHR System development lifecycle, enhances control of the system baseline(s) and increases cost avoidance.

The contractor shall:

a) Develop and provide a CCMIP (CDRL A035) in accordance with the PEO Configuration Management Plan and PEO Release and Deployment Management Plan

b) Execute CM activities and processes for establishing and maintaining consistency of the EHR System's design, configuration, and operational information throughout the system development lifecycle in accordance with the approved CCMIP (CDRL A035)

5.5.4.1 Engineering Change Process

The contractor shall:

a) Develop and submit Engineering Change Requests (ECRs) (CDRL A044) as possible changes are identified

b) Provide traceability to ECR requirements and configuration items (CI) for all delivered software

c) Record and track ECR numbers within the internal change management and development tracking systems throughout the system development lifecycle

   i. All work units tracked internally shall also be mapped to associated ECRs, requirements, and CIs

d) Provide the Government with access to the contractor's internal change management/ development tracking systems

5.5.5 Release Management

The contractor shall:

a) Perform release management activities in accordance with the approved CCMIP (CDRL A035)

b) Perform the following activities to develop the CCMIP, including, but not limited to:

   i. Planning, build, test, and deploy EHR System releases

   ii. Identify and manage risks to successfully deploy each EHR System release

   iii. Establish a common understanding of each EHR System release between the Functional, Business and Technical Stakeholders

   iv. Coordinate release with the system development lifecycle components: Engineering Management, Program/Project Management, Requirements Management, Development Management, Cybersecurity Management, Infrastructure Management, Logistics & Lifecycle Sustainment Management, Test Execution, Change and Configuration Management, Transition Planning, Scheduling, and Build and Deployment Management

5.5.6 Data Management

The contractor shall:

a) Develop and provide a Contractor Data Management Plan (CDMP) (CDRL A027) in accordance with the DHMSM EMP, DHMSM Interface Strategy, and the PEO Data Management Strategy

b) Perform the following activities to develop the Contractor Data Management Plan, including, but not limited to:

   i. Review and align data management activities to enable Government compliance with the DoD Instruction "Sharing Data, Information, and Information Technology

(IT) Services in the Department of Defense" (DODI 8320.02), which conveys the data management activities that must take place to enable net-centric concepts

ii. Review and align with the processes and guidance outlined in the DHMSM EMP and PEO Data Management Strategy

iii. Coordinate with the DHMSM PMO to engage with DMIX, DHA, and TMIP-J regarding data management strategies and activities for:

a. Access to clinical and patient health information

b. Data migration to support transition

iv. Provide a Contractor Data Management Plan (CDRL A027) that is consistent with the PEO Data Management Strategy to include, at a minimum, the following:

a. Identity and Access Management Architecture

b. Specifications for use of national standard clinical terminology (e.g. LOINC, RxNorm, etc.)

c. Guidelines for the use of standards for clinical data exchange

c) Perform data management and migration activities in accordance with the approved Contractor Data Management Plan (CDRL A027)

d) Not use any Government information for any purpose other than in performance of this contract

5.5.7 Cybersecurity

The contractor shall:

a) Provide cybersecurity that conforms to the DoD cybersecurity and the DoD Risk Management Framework requirements as outlined in the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) as virtually documented at http://iase.disa.mil/index2.html

b) Establish appropriate administrative, technical, and physical safeguards to protect all Government data, to ensure the confidentiality, integrity, and availability of Government data in accordance with the requirements specified in the subtasks below

c) Comply with all cybersecurity training and Joint Interoperability certification requirements, as delineated in DoD 8570.0-M

d) Provide a DoD 8570.01 Compliance Report (CDRL A039) including:

i. A list of cybersecurity functional responsibilities for contractor personnel, by category (e.g., technical or management) and level (e.g., computing environment, network environment, or enclave)

ii. The cybersecurity training, Joint Interoperability certification, Joint Interoperability certification maintenance, and continuing education or sustainment training required for the contractor cybersecurity functional responsibilities

iii. A matrix documenting and tracking Joint Interoperability certification status of contractor cybersecurity personnel, updated as Joint Interoperability certifications change or expire and personnel are added or removed

5.5.7.1 Certification and Accreditation (C&A)

The contractor shall:

a) Support the EHR System solution Certification and Accreditation (C&A) activities to include development of artifacts for the Security Authorization Package (CDRL A033).

b) Comply with all applicable cybersecurity standards and directives outlined in:

   i. The Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) site: http://iase.disa.mil/index2.html

   ii. The NIST references and security guidance found at NIST's Computer Security Resource Center site: http://csrc.nist.gov/

   iii. The USCYBERCOM orders and directives found at: https://www.cybercom.mil/J3/orders/default.aspx

c) Mitigate all security risks and vulnerabilities found during C&A and continuous monitoring activities in accordance with the DoDI 8510.01

5.5.7.2 Incident Management

The contractor shall:

a) Provide an Incident Management Plan (CDRL A025), including an Information Operations Condition (INFOCON), to meet the requirements in accordance with the Chairman of the Joint Chiefs of Staff Manual (CJCSM-6510.01B)

b) Execute the activities identified in the Incident Management Plan (CDRL A025) in the event of a cyber-incident

c) Analyze incidents and report results in a Technical Report (CDRL A038) to the Government-assigned Computer Network Defense Service Provider (CNDSP) and DHMSM PMO

d) Support any actions deemed necessary by CNDSP Tier 1 and Tier 2 in accordance with DoDD 8530.1

5.5.7.3 Cybersecurity Vulnerability Management (CVM)

The contractor shall:

a) Manage and deliver a Technical Report (CDRL A038) documenting the EHR System compliance with the CVM program in accordance with the PEO Cybersecurity Strategy

b) Manage and deliver a Cybersecurity Vulnerability Management Plan (CDRL A046) documenting the contractors processes, approach, plans, and methodology applicable to all Cybersecurity Vulnerabilities published by the DoD and United States Cyber Command (USCC)

5.5.7.4 Maintain Situational Awareness/Continuous Monitoring

A cybersecurity vulnerability is any flaw or weakness that could be exploited to gain unauthorized access to, damage, or otherwise affect the EHR System.

The contractor shall:

a) Perform continuous monitoring of the approved security baseline in accordance with the DoDI 8510.01

b) Mitigate all newly discovered vulnerabilities within the specified timelines based on Category level of the findings in accordance with DoDI 8510.01

c) Manage and deliver Cybersecurity Vulnerability Assessment (CVA) reports (CDRL A038) documenting the EHR System vulnerabilities

5.5.7.5 Annual Review Support

Once the Designated Approval Authority (DAA)/Approving Official (AO) has accredited the system, the contractor shall:

a) Support the EHR System annual reviews activities as defined in the references found on the IASE site

   i. Annual reviews shall be completed prior to one (1) year from the date of the last signature on the approved Security Authorization Package (CDRL A033)

   ii. Annual reviews shall include updates to the artifacts for the Security Authorization Package (CDRL A033) as required

5.5.7.6 Risk Assessments/Security Impact Assessments

The contractor shall:

a) Provide expertise to monitor the risk posture of the EHR System throughout the contract

b) Assess cybersecurity risks following an incident or identification of vulnerabilities that may impact the cybersecurity posture of the system

c) Document findings in a Cybersecurity Risk Assessment Report (CDRL A038)

5.5.7.7 Cybersecurity Compliance Validation

The Government will approve the cybersecurity baseline for the EHR System and the standard tools that will be used for the cybersecurity efforts. The DoD is in the process of transitioning from the DIACAP to the DoD Risk Management Framework (RMF) for IT assessment process.

The contractor shall:

a) Utilize the DoD RMF for IT processes unless directed by the Government to utilize DIACAP processes. DIACAP processes and documentation may be required for certain individual MTFs which have not yet transitioned to the DoD RMF for IT

b) Provide cybersecurity artifacts that demonstrate the EHR System compliance with the DoD cybersecurity requirements, as defined in the Security Authorization Package (CDRL A033)

c) Scan the environments and system components using a Government approved tool set

d) Conduct regular security scans and submit a Technical Report (CDRL A038) which includes Plan of Action and Milestones (POA&M) and identifies all vulnerabilities and proposed mitigations

   i. All vulnerabilities must be mitigated in accordance with DoDI 8510.01 based on Category level

e) Support Independent Government scan(s) of the EHR System and environments, review the Government findings summary reports, provide analysis regarding the variances, and rectify any variances as appropriate in future scans

f) Participate in quarterly cybersecurity Interim Program Reviews (IPRs)

   i. Review the vulnerability findings and receive Government direction for the management of the cybersecurity efforts throughout the cybersecurity lifecycle

   ii. Update the POA&M (CDRL A038) as appropriate

5.5.7.8 Personnel Requirements

In support of the cybersecurity program efforts, the contractor shall:

a) Provide a primary and secondary point of contact to the DHMSM PMO

   i. These individuals will be the points of contact (POCs) for receiving all cybersecurity notifications (e.g., IAVM messages, POA&M messages, C&A efforts, monthly reporting) and provide the acknowledgment of receipt of these notifications via email to the DHMSM PMO cybersecurity POC within two (2) business days, unless otherwise specified by the Government

b) Complete the efforts described by these notifications within the timeframes specified in the notifications

5.5.8 System Safety

The contractor shall:

a) Conduct a system safety engineering program tailored for an OTS software-intensive system in accordance with MIL-STD-882E and the DoD Joint System Safety Engineering Handbook

b) Develop and execute a SSP (CDRL A048) that includes the necessary planning, coordination and analysis to:

   i. Identify the safety significant functions (safety critical and safety related) of the system and establish a protocol of analysis, design, test, and verification and validation for those functions within the system development activities

   ii. Establish a system criticality assessment with a level of rigor that is protocol for the requirements, design, code, and test of safety-significant system functions

   iii. Tailor and communicate generic or initial system safety requirements or constraints to the system and software designers as early in the lifecycle as possible

   iv. Analyze the existing documented hazards to determine software influence on these hazards in terms of causal initiation or causal propagation

   v. Consider the system-level effects of each identified hazard

   vi. Provide input to system engineering as to the potential contributions or implications of the software that would affect probability of occurrence

   vii. Conduct in-depth analysis to identify each failure pathway and associated system causal factors. This analysis will be to the functional depth necessary to identify logical, practical, and cost-effective mitigation techniques and requirements for

each failure pathway initiator (causal factor). This analysis shall consider all potential hardware, software, and human factor interfaces as potential contributors

viii. Derive safety-specific hazard mitigation requirements to eliminate or reduce the likelihood of each causal factor within the software functional architecture

ix. Provide engineering evidence (through appropriate inspection, analysis, and test) that each mitigation system safety requirement is implemented within the design, and the system functions as required to meet the stated level of rigor, safety goals, and objectives of the program

x. Conduct a safety assessment of all residual safety risk after all design, implementation, and test activities are complete

xi. Conduct a safety impact analysis on all Software Change Notices, PTRs, or ECPs for engineering baselines under configuration management

5.6 Testing

The DHMSM Test Strategy emphasizes early user engagement and integrated test and evaluation by teaming multifunctional organizations through active participation in a Test Integration Work Group (TIWG). It documents the overall Test and Evaluation (T&E) approach that can be tailored for each BoS/BoB product to ensure operational, functional, and technical readiness. Test activities will be conducted in production-representative Government labs as outlined in the DHMSM Government-Approved Labs (GALs) Plan.

Segments 1 and Segment 2 testing occurs simultaneously within the following three phases: 1) Configuration and Integration Test (CIT), 2) Developmental Test and Evaluation (DT&E), and 3) Operational Test and Evaluation (OT&E).

The contractor shall:

a) Deliver a CMTP, a component of the Test Plan (CDRL A007), consistent with the DHMSM Test Strategy, which describes the contractor's testing approach and support.

   i. Maintain the CMTP, incorporating updates needed to reflect any changes

b) Provide previous test results for analysis to help the Government focus on testing on higher risk areas as they relate to the Government RTM. Previous testing consists of activities the contractor has conducted before contract award. The scope of previous testing may include, but is not limited to, business metrics, warranties, inspections, and surveys. The Government will determine if results of previous testing are satisfactory to validate specific requirements within the Government RTM (Attachment 2). The previous test results proposed by the contractor to satisfy requirements shall be included as an appendix to the CMTP, a component of the Test Plan (CDRL A007)

c) Populate the Government-approved electronic Test Data Repository. The Test Data Repository utilizes IBM Rational Jazz products and manages all test-related material to include, but is not limited to, the following as described in the CMTP (CDRL A007) and Test Report (CDRL A040):

   i. Test plans

   ii. Test reports

   iii. Test data sets

iv. User documentation

v. Test related system documentation

vi. Tests cases and associated results

vii. Automated and manual scripts

viii. Other test support items

ix. Existing defects

d) Lead CIT and support all necessary testing throughout DT&E and OT&E test phases to achieve approval for Full Deployment Decision ATP

e) Meet the entrance and exit criteria for each phase as described in the DHMSM EMP, DHMSM Test Strategy and approved CMTP, a component of the Test Plan (CDRL A007). Contractor test efforts shall include, but are not limited to, the following as described in the Test Plan (CDRL A007) and Test Report (CDRL A040):

i. Develop test plans, scripts, data, cases, and reports

ii. Provide access to the CIT lab facilities

iii. Respond to Government personnel regarding matters including testing scope, approach, timeline, testing processes, and tools

iv. Conduct testing as described in the Test Plan (CDRL A007)

v. Define the process for defect management and resolution, including re-testing

vi. Use automated tools that are interoperable with the DHMSM PMO's tools as defined in the DHMSM Test Strategy

vii. Assist in fault isolation and detail analysis of testing results

viii. Sustain the EHR System in test environments to include Help Desk and other operational services

f) Once Full Deployment is achieved, provide all aspects of testing to support the EHR System during operations.

5.6.1 Testing Meetings

The contractor shall:

a) To expedite CMTP approval, host and conduct a meeting with the Government as soon as practical, but no later than 30 days after issuance of the Task Order, to coordinate the contents of the CMTP

b) Provide Meeting Agendas (CDRL A002), Presentation Materials (CDRL A003), and Meeting Minutes (CDRL A004)

c) Participate in and provide documentation required for the DHMSM TIWG and formal reviews. Reference the DHMSM Test Strategy and DHMSM EMP

5.6.2 Integration and Test Lab Environment

The Government will use two types of GALs to serve as integration and test lab environments:

- Mockups of the medical operational environments in which end users will interact with the EHR System

- Test Data Center to represent the data centers that will support the EHR System.

The contractor shall at a minimum:

a) Implement and operate the EHR System in the GALs as defined in the DHMSM GALs Plan

b) Implement and operate the contractor's IDE (also referred to as the Contractor Sandbox in the DHMSM GALs Plan) in the GALs

c) Provide the Government with read access to the contractor's IDE (e.g., coding tools, build servers, code management and reporting systems, quality management system) necessary to independently validate development progress, assess quality, verify test status in support of SETRs and In-Process Technical Reviews throughout the EHR System Lifecycle

d) Provide hardware, software, and professional services required for installation, configuration, and interfaces of the EHR system in the GALs

e) Provide the necessary supply support (e.g., hardware spares, cabling, and test equipment) required for the repair of failed EHR System components. Normal expendable supplies such as paper (for reports), printer cartridges, and other items are the responsibility of the host site

f) Perform an asset audit upon completion of installation of the EHR System and document results in an Asset Audit Report (CDRL A018)

g) Install the EHR System in the GAL locations identified in the Task Orders

h) Provide, install, and configure test data sets in accordance with the Test Plan(s) (CDRL A007) for testing of the EHR System

i) Provide and refresh test data sets inherent to the EHR System as needed to verify that requirements are met

5.6.3 Configuration and Integration Testing

The contractor shall:

a) Contractor shall conduct Configuration and Integration Testing (CIT), consistent with the DHMSM Test Strategy, in the GALs providing the empirical evidence that all system requirements have been achieved and the EHR System is suitable for Government testing

b) Provide a Test Plan (CDRL A007) and Test Report (CDRL A040) for every test identified in the CMTP

c) Map the Government RTM requirements (Attachment 2) to test scripts and test results

d) Provide training to the Government testers and SMEs as defined in the Implementation Plan (CDRL A006)

e) Provide access during CIT for Government testers and IV&V agents for over-the-shoulder observation of contractor's testing, as necessary

f) Provide test scripts and test results through the Test Data Repository

g) Verify the EHR System meets all requirements defined in the RTM (CDRL A028) in accordance with the CMTP (CDRL A007)

h) Identify deficiencies, defects, and resolutions identified through testing in the Test Data Repository and:

   i. Use the defects severity and priority classifications defined in the DHMSM Test Strategy

   ii. Fix defects as required by the Government and conduct regression testing to verify the fix

i) Conduct a smoke test of the EHR System as described in the CMTP

j) Conduct data migration/conversion/performance testing in the GAL, and provide the results in the Test Report (CDRL A040)

k) Submit a close-out Test Report (CDRL A040), at the conclusion of CIT, identifying the tests completed for specific system criteria; test results, findings, and conclusions; test limitations, gaps, and impacts; identified risks and mitigations; and readiness to proceed with the Government DT&E

l) Participate in and provide documentation in support of the combined Test Readiness and Final Design Review (TRR/FDR) for entry into DT&E

   i. Demonstrate the achievement of entrance and exit criteria identified in the DHMSM EMP, DHMSM Test Strategy, and CMTP

   ii. Provide an agenda (CDRL A002), meeting minutes (CDRL A004), presentation materials (CDRL A003)

   iii. Demonstrate the EHR System's ability to meet criteria specified in the DHMSM EMP and the DHMSM Test Strategy to establish that the system design is stable, ready to enter Government test with acceptable risk, and to support Government establishment of an Initial Product Baseline captured in the EHR Technical Baseline Documents (CDRL A030)

   iv. Designate subject matter experts to participate in the meeting and address all agenda items

m) Deliver all items identified in CMTP, a component of the Test Plan (CDRL A007) upon completion of exercising them in the CIT

n) Provide a weekly and a daily current schedule, and a summary of the daily testing results addressing traditional software-project metrics such as, but not limited to, requirements identified by quantity and type, requirements scheduled to be tested by the end of each week (weekly and cumulative), requirements successfully tested, requirements resulting in defects identified to be corrected, and requirements for which the same defect is detected again after its correction has been reported

   i. Provide this information through the Government-approved electronic Test Data Repository

5.6.4 Developmental Test and Evaluation

During DT&E, Independent Government test agencies will verify the EHR System in the GAL. At the end of DT&E, the Operational Test Agency will conduct an Operational Test Readiness Review (OTRR) to determine whether to enter OT&E. To support the Government's testing of the EHR System, the contractor shall perform the technical services required for DT&E in accordance with the CMTP (CDRL A007) including, but not limited to, the following:

a) Support Government testing by providing the necessary tools, training, and application support for the EHR System

b) Train the Government testers, SMEs, and other user representatives as defined in the Implementation Plan (CDRL A006).

c) Provide support to resolve issues, fix defects, isolate faults, and analyze anomalies

d) Conduct regression testing as needed

e) Place all deliverables subject to DT&E under configuration control, which includes, but is not limited to:

   i. Software components

   ii. Hardware components

   iii. User and technical documentation

   iv. Training Materials (CDRL A024)

5.6.5 Operational Test and Evaluation

The Government will conduct OT&E at selected IOC sites for Segment 1 and GALs for Segment 2 as described in the DHMSM Test Strategy. The contractor shall perform the following activities in support of the Government's OT&E of the EHR System:

a) Provide the necessary tools, training, data, application support and services to accomplish operational testing of the EHR System in accordance with the CMTP (CDRL A007) and site-specific Implementation Plan (CDRL A006)

b) Train the Government testers, SMEs, and other user representatives as defined in the Implementation Plan (CDRL A006)

c) Provide problem resolution support to resolve issues, fix defects, isolate faults, and analyze anomalies

5.7 Deployment Services

The contractor shall:

a) Provide services and materials necessary to complete site preparation, deployment, and post-installation support

   i. Deployment activities will differ between Segment 1 and Segment 2 and be further defined in Task Orders

b) Provide the Implementation Plan (CDRL A006) that:

   i. Aligns with the DHMSM DTCMP and describes the strategy and approach for deployment, training, change management, and sustainment

   ii. Defines the Enterprise Deployment Wave Construct

   iii. Aligns to the region and Wave construct in the Segment 1 MTF List and MTF Codes (Attachment 12)

   iv. Supports TMIP-J and the Services Infrastructure Program Offices as they deploy the EHR System to the Segment 2 operational units in accordance with the Segment 2 Roles of Care and Descriptive Statistics (Attachment 13)

5.7.1 Deployment Site Visit

The contractor shall:

a) Travel to the specified Segment 1 sites and conduct site visits in accordance with the Implementation Plan (CDRL A006)

b) Develop an Agenda (CDRL A002) and Presentation Materials (CDRL A003) for each site visit

c) Conduct an EHR System demonstration

d) Develop and submit a site-specific Implementation Plan (CDRL A006)

   i. Develop a Wave-specific deployment schedule based on site visits that aligns to the checklist provided in the DHMSM DTCMP and submit as part of the Wave-specific Implementation Plan

   ii. Coordinate with MTF personnel to assign users to the new EHR System-defined roles and document the assignments in the Implementation Plan (CDRL A006)

   iii. Review the checklist provided in the DHMSM DTCMP and update the checklist to add contractor tasks required for deployment, training, change management, and sustainment

      a. Submit the initial checklist for Government approval as a part of the Implementation Plan (CDRL A006)

   iv. Track progress towards completing all items in the Government approved checklist and report status (e.g., percentage of tasks complete, outstanding tasks, risks associated with outstanding tasks, and risk mitigations plans) to the Government in the Monthly Progress Report (CDRL A008)

e) Participate in functional and non-functional working group meetings during the site visit

   i. Provide SME participation based on agenda items

f) Conduct a Business Process Workshop (or series of workshops, if needed)

   i. Present the Enterprise To-Be Business Process Workflows and user roles definitions in the Presentation Materials (CDRL A003)

   ii. Conduct gap analysis of site As Is workflows to the Enterprise To-Be to identify training and change management activities

   iii. Document gap analysis findings in the Site Visit Report (CDRL A041)

   iv. Update the Training Materials (CDRL A024) as necessary to reflect the updated workflows

g) Develop and submit a Site Visit Report (CDRL A041)

5.7.2 Segment 1 Training

The contractor shall:

a) Plan and execute instructor-led classroom, instructor-led virtual, CBT, and over-the-shoulder training, consistent with the DHMSM DTCMP and approved Implementation Plan (CDRL A006), in a manner that will meet the QASP performance standards

(Attachment 14) for training, facilitate user adoption and prepare users for successfully using the EHR System

b) Provide certification training to Services' training staff to enable them to train and certify other trainers and end users

c) Provide enhanced training to super users and clinical champions

d) Provide training to end-users including but not limited to the following personnel: functional, technical, administrative, and help desk staff

e) Administer competency tests and conduct User Experience Satisfaction Surveys in accordance with the Training Materials (CDRL A024). Report the percentage of users who have passed the competency test and summary of User Experience Satisfaction Surveys in the Monthly Status Report (CDRL A008)

f) Update the site training schedule in the Implementation Plan (CDRL A006) to accommodate Government directed changes. Upon Government approval, integrate the training schedule in the CIMS and submit it as part of the IPMR (CDRL A005)

g) Provide training to the Government testers and SMEs as defined in the Implementation Plan (CDRL A006)

5.7.3 Segment 2 Training

Any initial end-user training required for Segment 2 shall be in accordance with Section 5.7.2. This Section covers training of TMIP-J and individual Services' master trainers only. The contractor shall:

a) Provide certification training to TMIP-J and the Services' infrastructure program offices' Master Training and Fielding Teams

   i. Plan and execute instructor-led classroom, instructor-led virtual, CBT, and over-the-shoulder training

   ii. Enable TMIP-J and master trainers to train and certify other trainers and end users. Specific training sites will be designated by the DHMSM PMO in Task Orders

b) Administer competency tests and conduct User Experience Satisfaction Surveys in accordance with the Training Materials (CDRL A024). Report the percentage of users who have passed the competency test and summary of User Experience Satisfaction Surveys in the Monthly Status Report (CDRL A008)

5.7.4 Segment 1 Deployment

The contractor shall:

a) Manage, execute, and report on deployment activities as defined in the Implementation Plan (CDRL A006). Full Deployment (FD)/Full Operational Capability (FOC) must be achieved by the end of FY 2022

b) Travel to the locations identified in the Task Orders and conduct the following activities to install, configure, test and document site production hardware and software:

   i. Deliver the EHR System Installation Guide (CDRL A026)

   ii. Provide and install all hardware and software required to establish and maintain

the EHR System in the regional or centralized local production environment(s)

iii. Provide the services for establishing the EHR System production environment(s) as identified in the EHR System Installation Guide (CDRL A036)

iv. Implement site specific interfaces as identified in the Implementation Plan (CDRL A006)

v. Conduct site specific Data Migration in accordance with the RTM and Contractor Data Management Plan (CDRL A027)

vi. Prepare and present an Installation In-Brief (Installation Technical Documentation and Plans) (CDRL A002) to the Government Installation Manager

vii. Apply SW upgrades, tool extensions and templates to meet security or specific functionality requirements

viii. Perform site installations and post installation testing in accordance with the CMTP (CDRL A007)

c) Provision successfully trained users to the EHR System and confirm successful provisioning

d) Provide status updates on role provisioning to include the total number and percentage of end-users who have completed training in the Monthly Progress Report (CDRL A008)

e) Provide post Go-Live on-site sustainment and maintenance support to the MTFs to include:

i. Provide 24/7 on-the-job/over-the-shoulder support

ii. Troubleshoot, track, and resolve functional/technical incidents for end-users

iii. Report all end-user incidents and training trends in the Monthly Progress Report (CDRL A008)

iv. Proactively engage end-users to identify unreported functional/technical incidents and provide additional training as necessary

v. Modify Training Materials (CDRL A024) as necessary

f) Support the Post-Implementation Review activities as identified in the Implementation Plan (CDRL A006) in order to achieve a FDD

g) Develop a Training Schedule in the Implementation Plan (CDRL A006) for each deployment Wave

i. Upon Government approval, integrate training schedule in the CIMS and submit as part of the IPMR (CDRL A005)

5.7.5 Segment 2 Deployment

After Segment 2 has successfully completed Operational Testing and Evaluation in the GALs with environments representative of Operational Medicine capabilities for Role 1, Role 2, Role 3, and EnRoute Care the contractor shall execute and provide the following activities at the Government-identified Segment 2 site(s) in accordance with the Task Order(s):

a) Develop and deliver the EHR System “Gold-Disk” (CDRL A043) to include the following CDRLs:

i. System Subsystem Specifications (CDRL A020)
ii. System Subsystem Design Description (SSDD) (CDRL A021)
iii. Computer Software Products (CDRL A023)
iv. Training Materials (CDRL A024)
v. Interface Control Document (ICD) (CDRL A029)
vi. Database Design Description (CDRL A031)
vii. Security Authorization Package (CDRL A033)
viii. EHR System Installation Guide (CDRL A036)
ix. Version Description Document (CDRL A045)

b) Update and resubmit the Gold Disk as approved major, minor, maintenance, and patch baseline changes are implemented

c) Travel to locations identified in the Task Order(s) to assist TMIP-J and the Services with EHR System configuration, integration, implementation, site preparation, system setup and validation, and initial implementation training utilizing the EHR System Segment 2 Product Gold-Disk

d) Participate in recurring monthly Segment 2 Implementation and Deployment meetings through FD

5.8 Sustainment

DHMSM sustainment includes all manpower, maintenance, and support activities conducted by the contractor to ensure the operation and performance of the EHR System: this includes the sustainment of all laboratory and test systems from the implementation of CIT through the lifecycle of the system. A Segment 1 MTF enters sustainment no earlier than Go-Live and no later than completion of post-implementation/Go Live training. Segment 2 Sustainment begins with delivery and acceptance of the EHR System Gold Disk (CDRL A043). Segment 2 sustainment is a coordinated support-only effort between the contractor, DHMSM, DHA, and the Services' infrastructure program offices.

The contractor shall:

a) Provide all hardware, software, and services necessary to perform overall sustainment of the EHR System

b) Provide EHR System Segment 2 programmatic, engineering, training, and Help Desk support for implementation, system setup, maintenance and sustainment for TMIP-J and the Services

c) In accordance with the helpdesk functions and the system performance requirements contained in the DHMSM DTCMP and Government RTM, provide continuous technical support and system monitoring beyond CIT to immediately react to a system event

d) Report on the sustainment activities in accordance with the approved Implementation Plan (CDRL A006) and SEMP (CDRL A034) in the Monthly Progress Report (CDRL A008)

5.8.1 Software Maintenance

Software maintenance includes all releases of the software such as major releases, minor releases, maintenance releases, patches, cybersecurity, and software assurance updates as those terms are defined in the PEO DHMS Configuration Management Plan. Maintenance will be conducted in such a way to minimize impact to the user community.

The contractor shall:

a) Provide software maintenance and support for the EHR System. Maintenance support will be established for the EHR System before IOC and will continue throughout the DHMSM lifecycle

5.8.1.1 Configuration/Customization Maintenance

The contractor shall:

a) Maintain the EHR System and deliver updated software and documentation in accordance with the Computer Software Products (CDRL A023), the SDP (CDRL A032), and the SEMP (CDRL A034)

b) Maintain all EHR System interfaces identified in the CRTM (CDRL A028), including but not limited to, interfaces to DoD enterprise systems, local MTF medical devices and systems, DMIX legacy data services, DoD data warehouses/analytics/SOA, and external partners/organizations

c) Ensure that existing functionality of the EHR System is not compromised due to enhancements or updates unless specifically directed or approved by the Government

5.8.1.2 OTS Software License Maintenance and Renewal

The contractor shall:

a) Maintain OTS SW applications and tools

   i. Notify the Government of any software that will reach end of life, end of service, or end of SW maintenance release within two years

   ii. Ensure all OTS software has continuous vendor support

5.8.2 Hardware Maintenance

The contractor shall:

a) Maintain EHR System contractor-provided hardware in accordance with IDIQ PWS Section 5.2.3

b) Manage and maintain Government-Furnished Property (GFP) in accordance with IDIQ PWS Section 5.1.9

c) Provide the necessary supply support (e.g., hardware spares, cabling, and test equipment) required for the repair of failed EHR system components

d) Maintain all hardware in compliance with manufacturers' warranties

e) As required, de-install, move, and install EHR System computer hardware, excluding medical devices, in a manner that will not void warranties

f) Support hardware items once the commercial product warranties expire without voiding Return to Factory (RTF) warranties

5.8.3 Product Improvement Engineering

Product improvement changes include changes, additions, or new capabilities/products that provide for functionality upgrades or technology insertions. These changes maintain or expand interoperability or address obsolescence issues.

The contractor shall:

a) Conduct engineering changes in accordance with IDIQ PWS Section 5.5.4 and as detailed in individual Task Order PWSs

   i. Submit engineering change requests (ECRs) (CDRL A044)

b) Conduct Pre-planned Product Improvement (P3I) change architecture/design activities in accordance with the system design requirements of section 5.2.5 of this PWS and as documented within the CIMS (CDRL A005)

5.8.4 Software and Hardware Refresh

Technology refresh is the periodic replacement of HW, SW, and assigned non-IT assets (e.g., electrical panels and Heating, Ventilation, and Air Conditioning (HVAC)) to avoid obsolescence and loss of Original Equipment Manufacturer (OEM) support, improve reliability and availability, reduce the TOC, and remain current with Government security requirements and industry IT standards

The contractor shall:

a) Conduct technology refresh activities in accordance with the technology refresh requirements defined in TRP (CDRL A022)

5.8.5 Operations and Monitoring

Operations and Maintenance includes all the resources, processes, metrics, measurement approach, and systems necessary to:

a) Continually assess the state of compliance of the EHR System with the schedule, quality, performance requirements defined in the Government RTM (Attachment 2)

b) Assess the effectiveness of the EHR System's ability to ensure and enable sustainability, flexibility, and interoperability of the MHS while improving the continuity of patient care

c) Take proactive steps to determine and implement improvements to the level of services delivered

5.8.5.1 Help Desk Support

The contractor shall:

a) Receive, analyze, resolve, implement and close out all Tier 2.5 for Segment 2 and Tier 3 for Segment 1 trouble tickets issued by the DHA Global Service Center (DHAGSC)

b) Interface closely with the DHAGSC triage process, providing all information and updates to support the triage process, including ticket grouping, severity assignment, categorization and classification

c) Participate in the process for on-boarding the EHR System into the DHAGSC Help Desk

   i. Provide the Government with information required to complete the Operations and Infrastructure (O&I) Requirements Worksheet and the DHA Global Service Center Discovery Questionnaire

   ii. Communicate all EHR System updates, including hardware and software, to the DHAGSC Help Desk

   iii. Make SMEs available to support Help Desk staff

d) Provide 24/7 Tier 3 support for Segment 1 and Tier 2.5 support for Segment 2 to the DHA Global Service Center in accordance with the DHMSM DTCMP

   i. Provide technical troubleshooting and fixes for trouble tickets that cannot be resolve by DHAGSC support staff

   ii. Contact the network service provided for all Tier 3 access issues that cannot be resolved remotely

e) Use the current DHAGSC Incident Management Tool (Remedy) to enter; record status updates; and resolve DHAGSC application and system incidents (also called trouble tickets)

f) Receive, log, and track Tier 2.5 for Segment 2 and Tier 3 for Segment 1 trouble tickets via the DHAGSC triage process, and when appropriate, directly from the DHAGSC

   i. The tickets will address any software/hardware contained in the EHR system

   ii. DHAGSC reserves the right to implement a different trouble ticket management tool at any time

   iii. Any ticket issued with patient safety implications will be fast tracked and resolved as quickly as possible

   iv. Any ticket identified by the contractor to have patient safety implications not already identified as such must be reported back to DHAGSC triage immediately, and fast tracked as above

g) Respond to incident tickets within criticality response times as defined in Section 7.6.2.1 (DHAGSC Priority Levels) of the DHMSM DTCMP

h) Provide number and trends in tickets in the Monthly Progress Report (CDRL A008)

5.8.5.2 Sustainment Training

The contractor shall:

a) Provide ongoing sustainment support, including but not limited to, training EHR System users, maintaining training materials, supporting business process reengineering and change management efforts

   i. Provide an Implementation Plan (CDRL A006) to propose a regional team structure

b) For Segment 1 and Segment 2, provide training to training staff which includes:

i. Certification Training

ii. Training for software patches, updates, and new releases

iii. Optimization Training in accordance with section 7.4.8 of the *DTCMP*

c) Deliver updated EHR System Training Materials (CDRL A024)

d) Maintain and update the VTE to reflect any updates to the production environment

e) Provide additional training as directed by the Government, such as, but not limited, to surge training and mobile training

f) Continuously assess industry best practices and recommend improvements for the most efficient and effective business workflows for the EHR System

g) Participate in the Business Process Reengineering (BPR) IPT

h) Conduct a comparative analysis between the current EHR System workflows and the organizational business processes identified in the DoD Architecture Framework (DoDAF) Operational Viewpoint OV-6c Event Trace Descriptions and provide recommendations on process re-engineering, change management, and product configuration

i) Update the Business Process Workflow Diagrams and Role Definitions (CDRL A026) that define business and clinical workflows and describe functionality, improved efficiency, how meaningful use has been achieved, and establish EHR System user role definitions

j) Update the Role Assignment Identification Document (CDRL A042) that maps Segment 1 and Segment 2 user roles to EHR System roles

5.8.5.3 Sustainment Engineering

Sustainment engineering comprises those engineering and product support tasks that ensure the continued operation of the system and its supporting infrastructure. This includes the compilation of system problem reports; failure modes and effects analysis; system behavior trend analysis (e.g., reliability, maintainability, etc.); root cause analysis; development and testing of required engineering and product change proposals to modify the system configuration; conducting all testing in support of Cybersecurity Certification & Accreditation; and, other activities required to ensure the continued operation of the system and its supporting infrastructure.

The contractor shall:

a) Conduct sustainment engineering of the developed and operational system, from CIT onward through its life cycle.

b) Compile, maintain, and submit system problem reports and system performance statistics in the Monthly Progress Report (CDRL A008)

c) Ensure the Test Plan (CDRL A007) assess the EHR System's ability to meet all DHMSM performance requirements in the Government RTM (Attachment 12)

d) Enable the EHR System design to identify timing budgets for each of the major core system functions (see DHMSM EMP Section 2.7) to measure the impact of core system functions on overall performance and provide an approach to monitor and test overall

system responsiveness using GFP and contractor monitoring capabilities, in accordance with the PWS Section 5.2.9.e

e) Maintain updated failure modes and effects criticality analysis for all system components, including software

f) Maintain updated data and trend projections of maintainability, availability and other system attributes defined in the Government RTM

g) Conduct in-depth root cause analysis on system problem reports, document as CDRL A038 upon government request, identifying problem source and recommending resolutions for implementation

h) Develop and test modifications to the system configuration to include the following:

   i. Changes in the EHR System configuration, including new or modified hardware, software, ECRs, and patches

   ii. Segment 2 EHR System Gold Disk (CDRL A043) for all required patches and updates

   iii. Planned EHR System changes and of any emergency/urgent system changes using procedures in the SEMP (CDRL 034)

   iv. Document test results in the Test Report (CDRL A040)

   v. Report any incompatibilities with the current configuration in accordance with the CCMIP (CDRL A035)

   vi. Conduct SCQC activities in accordance with the PWS Section 5.5.2.1

i) Conduct cybersecurity activities in accordance with the PWS Section 5.5.7

j) Ensure the continued operation of the EHR System and its supporting infrastructure:

   i. Support the design, maintenance, failover testing, and rollback plans for EHR System for secondary and disaster recovery sites

k) Integrate continuous system monitoring with DoD support organizations (e.g. DISA, Service network operation centers, GALs, and MTFs). Integration activities include, but are not limited to:

   i. Work in conjunction with DHMSM PMO to establish Service Level Agreements (SLAs) with the DoD support organizations necessary for end-to-end system support

   ii. Establish system interfaces with the DoD Support Organizations, private and infrastructure monitoring systems and processes necessary for end-to-end system support

   iii. Monitor software and hardware performance required to support daily operations and reporting requirements per Government RTM (Attachment 2)

   iv. Identify root cause and impacts beyond the system’s boundary with recommendations for resolution

   v. Notify the Government of system issues using procedures defined in PWS Section 5.8.5.1

5.8.5.4 Sustainment Testing

The contractor shall:

a) Provide support for the EHR System in the GALs in accordance with IDIQ PWS Sections 5.6.4 and 5.6.5

   i. Sustainment includes the development of test artifacts (e.g. test scripts, test cases, test data sets, interface emulators) necessary to support the Configuration Control Board (CCB) with regression testing

   ii. Segment 2 sustainment includes support to TMIP-J and Services for the EHR System and interfaces, including the GALs during IOT&E

b) Provide the necessary tools, training, data, application support, regression testing and services to accomplish testing for sustainment engineering of the EHR System at the GALs